UIC John Marshall Journal of Information Technology & Privacy Law

Volume 29
Issue 1 *Journal of Computer & Information Law - Fall 2011*

Article 2

Fall 2011

The Amended EU Law on ePrivacy and Electronic Communications after its 2011 Implentation; New Rules on Data Protection, Spam, Data Breaches and Protection of Intellectual Property Rights, 29 J. Marshall J. Computer & Info. L. 29 (2011)

Vagelis Papakonstantinou

Paul de Hert

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.

VAGELIS PAPAKONSTANTINOU*
PAUL DE HERT**

Telecommunications are privileged in being the only sector in European Union ("EU") law benefiting from sector-specific data protection legislation. Although the (European) right to data protection is by now a fundamental right[1] intended to find horizontal application into any and all fields that involve even the remotest personal data processing, certain sectors did go ahead and acquire regulations, of various legal statuses, specific to their needs and special conditions. Telecommunications (electronic communications) have benefited from sector-specific data protection legislation since 1997, when the first relevant set of regulations was released. Today, the Directive on Privacy and Electronic Communications (the "ePrivacy Directive")[2] governs the field; its latest amendment, in 2009, brought forward the third in chronological (if not in generational) order relevant regulations.

* Partner at the MPlegal law firm in Athens, Greece, and researcher at the Brussels University (VUB-LSTS)

** Professor at the Brussels University (VUB-LSTS) and Associated Professor at Tilburg University (TILT)

1. *See* Consolidated Version of the Treaty on the Functioning of the European Union art. 16, May 9, 2008, 2008 O.J. (C 115) 47 (hereinafter "TFEU"); Treaty on European Union art. 39, Feb 7, 1992, 1992 O.J. (C 191) 1 (as in effect 1992) (now TFEU art. 38).

2. 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, 2002 O.J. (L 201) 37 (hereinafter "Directive on Privacy and Electronic Communications").

The latest EU Law in the field – Directive 2009/136/EC[3] – amended certain parts of the 2002 ePrivacy Directive,[4] which had in turn replaced the 1997 ePrivacy Directive.[5] Personal data protection was enhanced through the introduction of mandatory notifications of data breaches, reinforced protection against spyware or cookies, and even the possibility for any person negatively affected by spam, including Internet Service Providers ("ISPs" or "service providers"), to bring legal proceedings against spammers.

Two points should always be kept in mind while assessing the amended ePrivacy Directive from a data protection point of view. The first refers to the fact that the Directive itself is of a technical, complementary character. The ePrivacy Directive is particular to the needs and circumstances of the telecommunications sector. It does not introduce new fundamental data protection rules, but merely specifies and makes concrete in the telecommunications context the data protection principles set elsewhere (for the time being, in the Data Protection Directive[6]). Therefore, it cannot, by definition, be too detrimental or too positive for individual data protection, being obliged to observe the general rules and principles of the Data Protection Directive.

The second point refers to its fundamental limitation in scope. As a general rule, the ePrivacy Directive is addressed only to electronic communications service providers and not to information society service providers. Therefore, all Internet-related (e-commerce) activities are expected to escape its provisions. Perhaps itself acknowledging this limitation, the ePrivacy Directive attempts to break these asphyxiating boundaries and indeed regulate certain Internet activities (for instance, spam or cookies), seemingly trotting outside its scope. However, the

3. Directive 2009/136/EC, of the European Parliament and of the Council of 25 November 2009, *amending* Directive 2002/22/EC on Universal Service and Users' Rights Relating to Electronic Communications Networks and Services; Directive on Privacy and Electronic Communications; Regulation (EC) No 2006/2004 on Cooperation Between National Authorities Responsible for the Enforcement of Consumer Protection Laws, 2009 O.J. (L 337) 11 (hereinafter "2009 Amending Directive").

4. The consolidated text (including amendments by Directive 2006/24/EC on data retention) of which remains in effect today. Therefore, for the sake of clarity, references to the "ePrivacy Directive" in this paper, unless set otherwise, refer to this consolidated text, while the three regulatory texts under discussion shall be denoted as 1997 ePrivacy Directive, 2002 ePrivacy Directive, and 2009 ePrivacy Directive, respectively.

5. The ePrivacy Directive, although a standalone piece of legislation itself, forms part of the EU Telecommunications Regulatory Package; that is, a set of one Regulation and six Directives. A complete, consolidated list, as well as relevant information, may be found at the European Commission Information Society and Media Directorate General website.

6. 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 (hereinafter "Data Protection Directive").

above general rule is expected to create substantial difficulties while implementing its provisions in practice.

The purpose of this paper is to elaborate upon the merits of the amendments introduced by the 2009 ePrivacy Directive in the contemporary EU data protection environment. Perhaps unjustifiably, these amendments attracted little academic or other attention within and outside Europe. The ePrivacy Directive's May 25, 2011 implementation deadline largely passed unnoticed,[7] despite the fact that certain of its innovations have in the meantime gained enough influence to have directly affected general EU (or even global) data protection regulations. Our descriptive analysis will allow one to reflect about a classic problem in technology regulation, namely that of the added-value of specific tailored regulation as opposed to general regulation. Does this kind of sector-specific legislation, that is generally believed to be a lawmaking best practice in the data protection field, live up to its expectations, and is it indeed an effective lawmaking policy, at least from an individual rights point of view? The ePrivacy Directive has already been amended three times since 1997. This periodicity of review, although beneficial as far as technological advances are concerned, does not seem to allow for the necessary time to properly assess the effectiveness of legislative provisions for individual data protection. It is therefore not clear whether such frequent legislative review benefits individual data protection. For instance, the Data Protection Directive, an all-encompassing text, has not been reviewed since its release in 1995.

Because all three versions of the ePrivacy Directive are close in chronological order and succeed one another following technological and regulatory trends, it is essential, before elaborating upon its amendment and effect on European data protection, to first briefly highlight those aspects of its predecessors that demonstrate the development of issues that remain relevant today and their respective regulatory approaches over time. In sections 1 – 6 we will therefore briefly present the EU data protection framework preceding the introduction of the 2009 ePrivacy Directive, as well as the general regulatory environment upon which its specialized provisions build. Special emphasis will be given to the originally intended regulatory model of implementing sector-specific regulations to complement the general provisions, a model, however, that appears to have been ultimately employed only in the telecommunications sector. In addition, attention shall be given to the general EU data protection framework currently in reform, and the effect such reform may have for the ePrivacy Directive. Sections 7 and 8 describe the pre-

7. *See, e.g., Governments 'not ready' for new European Privacy Law*, BBC (Mar. 9, 2011, 02:55 AM), http://www.bbc.co.uk/news/technology-12677534 (hereinafter "*Governments*").

paratory phases and the background leading up to the introduction of the 2009 ePrivacy Directive. In sections 9-12 the focus is turned to those additions to the ePrivacy Directive that are considered of particular interest, at least from a data protection point of view. In this context, the cases of system integrity, spam, cookies and user consent, public directories, and personal data breach notifications are examined respectively. Finally, in section 13, special attention is given to the Three Strikes Law debate and to the Internet Freedom provision ultimately adopted in the text of the 2009 ePrivacy Directive.

1. SETTING THE BACKGROUND: GENERAL VERSUS SPECIFIC DATA PROTECTION REGULATIONS

In the EU, the data protection right is regulated in a "technical" vein. The regulations formulate conditions under which processing is legitimate, force a set of concrete obligations upon data controllers, and confer a set of processing-specific rights to individuals.[8] Because of its "technical" character and the fact that personal data processing is by now ubiquitous, it is also meant to be sector-specific.[9] Its principles and individual rights are intended to be incorporated through specialized regulations into each field of processing activities. However, the means of such customization may vary. In fact, concretization is by now achieved at Member State level through a wide array of instruments ranging from *soft law* (for instance, codes of practice or impact assessments) to specialized legislative texts.[10]

Today, the EU telecommunications sector is the only sector privileged to have specialized data protection legislation. Since the early 1990s, when it was formulated as an independent field of business and thus attracted the attention of lawmakers, it has always been accompanied by case-specific data protection regulations that closely tracked technological developments. Admittedly, the purpose of such legislation is two-fold: apart from data protection purposes, it also serves to protect the confidentiality of communications. However, it could be held that the latter is rather a secondary target; only a handful of relevant provisions

8. This is particularly of note when contrasted to the right to privacy; *see* Paul de Hert & Serge Gutwirth, *Data Protection in the Case Law of Strasbourg and Luxembourg: Constitualisation in Action*, in REINVENTING DATA PROTECTION? 3, 4 (Serge Gutwirth et al. eds., 2009). Data protection is not prohibitive for data processing, but rather sets concrete rules in order for it to be lawful. *Id.*

9. *See, e.g.*, ULRICH DAMMANN & SPIROS SIMITIS, EG-DATENSCHUTZRICHTLINIE, KOMMENTAR 65 (1997) (original in German); IAN J. LLOYD, INFORMATION TECHNOLOGY LAW 204 (4th ed. 2004).

10. VAGELIS PAPAKONSTANTINOU, SELF-REGULATION AND THE PROTECTION OF PRIVACY 91 (2002).

may be found in the respective texts,[11] and even in this case they are adapted onto already established data protection schemes and concepts.[12] In addition, confidentiality of communications is left out of the formal declaration of the relevant instruments' scope.[13] This treatment is perhaps unique to telecommunications, as no other personal data processing sector has been regulated until today so extensively by specialized data protection legislation.[14]

In order to properly set the scene that led to the latest amendment of the ePrivacy Directive and assess its contribution to EU data protection both from a substantive and a lawmaking point of view, the relationship between general EU data protection, currently under review, and sector-specific telecommunications regulations needs to first be highlighted. The retrospective analysis of more than twenty years of intensive regulatory effort will afford a clearer view as to the tensions and difficulties that the latest amendment attempted to address as well as to the effectiveness of the solutions adopted.

2. A SHORT SKETCH OF THE GENERAL EU DATA PROTECTION FRAMEWORK AND ACTORS

After the Lisbon Treaty entered into force on December 1, 2009, the right to data protection became expressly acknowledged in the Treaty on the Functioning of the European Union.[15] The same right is equally acknowledged in Article 8 of the European Convention for the Protection of

11. *See, e.g.*, Directive on Privacy and Electronic Communications, art. 5.3.

12. In particular, individual consent and the right to information. *See id.* at paras. 1, 3, and 5.

13. *See id.* at art. 1.

14. For instance, security processing (a sector admittedly much wider than telecommunications) only recently, in 2008, acquired horizontal legislation; although, certain subfields (PNR processing, Schengen, Europol, Eurojust) do benefit from specialized regulations. In a more closely related example, the banking sector knows, to date, no special data protection regulations (apart, perhaps, from those decisions formulating the SWIFT case). Marketing and insurance processing are, for the most part, regulated by codes of practice of various legal statuses. 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, 2008 O.J. (L 350) 60, 60-71; *see, e.g.*, Article 29 Data Protection Working Party, Opinion 4/2010 on the European Code of Conduct of FEDMA for the Use of Personal Data in Direct Marketing, 00065/2010/EN, WP 174, July 13, 2010.

15. TFEU at 47 ("Everyone has the right to the protection of personal data concerning them. The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent authorities.").

Human Rights and Fundamental Freedoms.[16] This constitutional acknowledgement is the culmination of a process that began in Europe in the 1960s.[17]

By the early 1990s, all EU-15 Member States (with the exception of Italy and Greece) had introduced data protection acts at the national level. In 1995 the EC adopted the Directive on the Protection of Personal Data (the "Data Protection Directive"), which, in effect, incorporated the main data protection regulatory solutions and schemes of national acts implemented up to that date.[18] The 1995 Data Protection Directive by now constitutes the basic data protection text within the EU. All EU Member States have incorporated its provisions into their national data protection acts; its principles and basic set of rights constitute the basis for all EU data protection discussions.[19]

In brief, the Data Protection Directive regulates the processing of personal data (defined as any information relating to an identified or identifiable natural person)[20] by laying down guidelines determining when the processing is lawful and prohibiting the processing of special categories of data (e.g. personal data revealing racial or ethnic origin,

16. "Everyone has the right to respect for his private and family life, his home and his correspondence." Article 8, par. 1, Council of Europe, Convention for the Protection of Human Rights and Fundamental Freedoms, *as amended* by Protocols No. 11 and No. 14. The European Court for Human Rights, based in Strasbourg, has assessed, while enforcing the Convention, a right to data protection from the right to privacy, which is actually directly referred to in Article 8; *see*, *e.g.*, de Hert & Gutwirth, *supra* note 8, at 3-44.

17. *See, e.g.*, FRITS W. HONDIUS, EMERGING DATA PROTECTION IN EUROPE (1975); DAVID H. FLAHERTY, PROTECTING PRIVACY IN SURVEILLANCE SOCIETIES: THE FEDERAL REPUBLIC OF GERMANY, SWEDEN, FRANCE, CANADA, AND THE UNITED STATES (1989); COLIN J. BENNETT, REGULATING PRIVACY: DATA PROTECTION AND PUBLIC POLICY IN EUROPE AND THE UNITED STATES (1992); 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, 123 (Martin Maik ed. 2008), *available at* http://www.vub.ac.be/LSTS/pub/Dehert/224.pdf.

18. *See* DAMMANN & SIMITIS, *supra* note 9, at 68.

19. In order to draw a complete picture, some reference must unavoidably be made to the (pre-Lisbon Treaty) Pillar system of the EU. The Data Protection Directive could only regulate processing of the so-called First Pillar, that is, commercial processing. All Third Pillar processing (security processing) was not affected, at least directly, by its provisions; such processing is currently regulated by the Data Protection Framework Decision. For a relevant analysis, *see* Vagelis Papakonstantinou & Paul de Hert, *The PNR Agreement and Transatlantic Anti-Terrorism Co-Operation: No Firm Human Rights Framework on Either Side of the Atlantic,* 46 COMMON MARKET L. REV. 885-919 (2009). However, the ratification of the Treaty of Lisbon, which abolished the Pillar system, is expected to bring grave changes to this system in the future. At any event, for the purposes of this paper, telecommunications processing is considered commercial processing falling under First Pillar processes and is thus regulated by the Data Protection Directive.

20. "An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity." Data Protection Directive, art. 2.

political opinions, religious or philosophical beliefs, trade-union membership, and of data concerning health or sex life as described in Article 8). The Data Protection Directive specifies the type of information to be given and the rights of individuals with regard to such information. It establishes a series of other guidelines concerning the quality of the data, the legitimacy of the data processing, individuals' right of information, access to data, the right to object to the processing of data, confidentiality and security of processing, the notification of processing to a supervisory authority, and the right to judicial remedy.[21] Transfers of personal data from a Member State to a third country are authorized only if the third country can guarantee an "adequate" level of protection.[22] Member States are also asked to provide that a public authority (also known as a "Data Protection Authority" or "DPA") monitors the application within their territory of the provisions adopted pursuant to it.

Article 29 of the Data Protection Directive established the Data Protection Working Party ("Article 29 Working Party"), a body that consists of representatives from all national DPAs and European Commission (the "Commission") officials (*cf.* the Article 29 from which it derives its name). The Article 29 Working Party aims to, among others, 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," but it has ultimately decided to rather act as a watchdog for EU data protection in general.[23]

In 2004, the position of the European Data Protection Supervisor ("EDPS") was established.[24] The EDPS, who is also a member of the Article 29 Working Party, is mainly responsible for monitoring the application of the Data Protection Directive provisions to all processing operations carried out by a European Community ("Community") institution or body. According to the relevant mission statement, the EDPS tasks are supervisory, consultative, and cooperative.[25] However, the EDPS has adopted, to date, an expansive approach as well, particularly

21. *See id.* at arts. 6, 7, 10, 11, 12, 14, and 16.

22. *See id.* at art. 25.

23. *See* de Hert, *supra* note 17, at 133.

24. Regulation (EC) No 45/2001 of the European Parliament and of the Council, of 18 December 2000 on the Protection of Individuals with Regard to the Processing of Personal Data by the Community Institutions and Bodies and on the Free Movement of Such Data, 2001 O.J. (L 8) 1; *see also* Peter Hustinx, European Data Protection Supervisor, *Data Protection in the Light of the Lisbon Treaty and the Consequences for Present Regulations*, 11th Conf. on Data Protection & Data Security – DuD 2009, Berlin (June 8, 2009), *available at* http://www.edps.europa.eu/EDPSWEB/webdav/shared/Documents/EDPS/Publcations/Speeches/2009/09-06-08_Berlin_DP_Lisbon_Treaty_EN.pdf.

25. *See* the EDPS website, http://www.edps.europa.eu.

with regard to his consultative tasks,[26] and has thus become an important, institutional actor in all data protection initiatives.

A final point of attention refers to the European Commission itself. General data protection is regulated by the Directorate General for Justice; whereas telecommunications, including telecommunications data protection, is regulated by the Directorate General for Information Society and Media. The two different Directorate Generals ("DGs") not only create some bureaucratic difficulties but, perhaps more importantly, reflect different approaches to data protection altogether. The DG for Justice allegedly places a stronger emphasis on the "security" part of its title these days, whereas the DG for Information Society caters, by definition, more to the market and individuals.[27]

The EU data protection regulatory framework is undoubtedly a complex one, making the task of correctly implementing its provisions far from straightforward.[28] After the Lisbon Treaty came into effect, the situation was supposed to be rationalized, but, nevertheless, this is not expected to happen in the immediate future. In the meantime, the transitory period is expected to cause additional difficulties.[29]

For the purposes of this paper, it is the provisions of the 1995 Data Protection Directive that set the groundwork for the specialized data protection telecommunications legislation that was introduced in 1997 and amended in 2002 and 2009. Notwithstanding the (by now obsolete) Pillar system, the Data Protection Directive constitutes the general and basic regulatory framework, upon which the ePrivacy Directive builds and whose provisions it makes concrete and specific in the telecommunications data processing sector.

The timing is, however, unique in the sense that, since November 2010, the Data Protection Directive has itself been undergoing an amendment process, the first in it's more than fifteen years of life.[30] In

26. An approach, however, justified by case law of the European Court of Justice; *see* Joined Cases C-317/04 & C-318/04, European Parliament v. Council of the European Union and Commission of the European Communities, 2006 O.J. (C 178) 1.

27. Indeed, data protection as a whole used to be regulated by the DG for Internal Market until 2005, when it was taken away from it and brought under the purview of the DG for Justice and Home Affairs (Justice only, as of July 1, 2010), a change that was (probably justifiably) much lamented by data protection proponents (*see infra*, Section 8). However, the Commission's restructuring appears interminable – by mid-2012, the DG for Information Society and Media was renamed "Directorate General for Communication Networks, Content, and Technology" ("DG Connect").

28. *See* SPIROS SIMITIS, DER VERKURZTE DATENSCHUTZ: VERSUCH EINER KORREKTUR DER DEFIZITE UND DISKREPANZEN IM JUSTITIELLEN UND SICHERHEITSBEREICH DER EUROPAISHCEN UNION 20 (2004) (original in German).

29. *See e.g.*, Hustinx, *supra* note 24.

30. *See European Commission Communication, A Comprehensive Approach on Personal Data Protection in the European Union*, COM (2010) 609 final (Nov. 4, 2010), *availa-*

early 2012, the Commission released its first proposal for the reform – overhaul in fact – of the general EU data protection framework;[31] as far as the ePrivacy Directive's subject matter is concerned, the Data Protection Directive is to be replaced by a General Data Protection Regulation ("Regulation").[32] Although this amendment process may well take years to conclude and its outcome is quite unpredictable, given the stakes at play, it appears that it will gravely affect the ePrivacy Directive. In fact, a number of the ePrivacy Directive's novelties discussed in this paper, such as data breach notifications, have been adopted by the draft Regulation and are expected thus to be raised to general personal data processing requirements.[33] On the other hand, a number of other novelties introduced by the Regulation, such as the "right to be forgotten," the right to "data portability," or the obligation for data protection impact assessments, may well have a direct effect upon ePrivacy Directive recipients, regardless of the *lex generalis/specialis* relationship. In addition, the Regulation appears to adopt an expanded notion for "personal data" and also affects certain basic notions, such as "individual consent," upon which the ePrivacy Directive also builds. It should also be noted that the Regulation, by definition, grants central controlling powers to the Commission rather than to national DPAs, purporting thus to make national data protection regulatory implementations obsolete. Consequently, once the Commission's reform work is concluded, the relationship between the ePrivacy Directive and the General Data Protection Regulation will most likely need to be re-examined and the added value of the former properly re-assessed.[34]

3. AN HISTORICAL SKETCH OF THE EU ELECTRONIC COMMUNICATIONS PRIVACY FRAMEWORK

Discussions on telecommunications[35] at the EU level only opened up

---

ble at http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_en.pdf (hereinafter "*European Commission Communication*").

31. *See* the relevant microsite, *available at* http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm.

32. *See* Press Release, European Data Protecting Supervisor, EDPS Welcomes a "Huge Step Forward for Data Protection in Europe", but Regrets Inadequate Rules for the Police and Justice Area (Jan. 25, 2012), *available at* http://europa.eu/rapid/pressReleasesAction.do?reference=EDPS/12/2&format=HTML&aged=0&language=EN&guiLanguage=en.

33. *See also* Paul de Hert & Vagelis Papakonstantinou, *The Proposed Data Protection Regulation Replacing Directive 95/46/EC: A Sound System for the Protection of Individuals*, 28 COMPUTER L. & SECURITY REV. 130-142 (2012).

34. *Id.*

35. The term "telecommunications" is no longer used in formal EU regulatory texts. Since 1999, telecommunications are regulated under the term "electronic communications" in the context of the "information society" strategy. After its first review, the telecommuni-

as late as the mid-1980s.[36] In 1993, the EU and its Member States committed themselves to the liberalization of the European telecommunications services sector by January 1, 1998.[37] This was performed primarily by means of enactment of a series of Directives having as their objective the opening up of the market (that was by then dominated by state monopolies) and the creation of a single market for telecommunications services in Europe.[38] The set of these Directives, which included the first version of the ePrivacy Directive,[39] came (retrospectively) to be known as the First Telecoms Legislative Package.

The increasing convergence of technologies (in effect, telecommunications and the Internet), as well as the fact that by then a number of Directives regulated the field that nevertheless did not always constitute a coherent and consequent framework, forced the Commission soon enough to propose a first review of the First Telecoms Legislative Package.

In 2000 a draft of the new telecommunications framework was launched. The regulatory framework was adopted on April 24, 2002, and entered into force in July 2003. It consisted of six Directives and one

---

cations regulatory framework formally transformed into the electronic communications regulatory framework.

36. *See European Commission, Towards a Dynamic European Economy: Green Paper on the Development of the Common Market for Telecommunications Services and Equipment,* COM (1987) 290 final (June 30, 1987).

37. *European Commission, Towards a New Framework for Electronic Communications Infrastructure and Associated Services, The 1999 Communications Review*, COM (1999) 537 final (Nov. 10, 1999) (hereinafter "*The 1999 Communications Review*").

38. The First Telecoms Legislative Package (mainly) consisted of: Commission Directive 94/46/EC, of 13 October 1994, *amending* Directive 88/301/EEC and Directive 90/388/EEC in Particular with Regard to Satellite Communications, 1994 O.J. (L268) 15 (hereinafter "Satellite Directive"); Commission Directive 95/51/EC, of 18 Oct 1995, *amending* Directive 90/338/EEC with Regard to the Abolition of the Restrictions on the Use of Cable Television Networks for the Provision of Already Liberalized Telecommunications Services, 1995 O.J. (L 256) 49 (hereinafter "Cable Directive"); Commission Directive 96/19/EC, of 13 March 1996, *amending* Directive 90/338/EEC with Regard to the Implementation of Full Competition in Telecommunications Markets, 1996 O.J. (L 74) 13 (hereinafter "Full Competition in Telecommunications Market Directive"); Directive 97/51/EC, of the European Parliament and of the Council of 6 October 1997, *amending* Council Directives 90/387/EEC and 92/44/EEC for the Purpose of Adaptation to a Competitive Environment in Telecommunications, 1997 O.J. (L 295) 23 (hereinafter "Competitive Environment Directive"); Directive 97/33/EC, of the European Parliament and of the Council of 30 June 1997 on Interconnection in Telecommunications with Regards to Ensuring Universal Service and Interoperability Through Application of the Principles of Open Network Provision (ONP), 1997 O.J. (L 199) 32 (hereinafter "Universal Service Directive").

39. Directive 97/66/EC, of the European Parliament and of the Council of 15 December 1997 Concerning the Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector, 1998 O.J. (L 024) 1 (hereinafter "Processing Directive").

Regulation.[40] This Second Telecoms Legislative Package, as amended in 2009, remains in effect today.

As per a statutory requirement in the Second Telecoms Legislative Package, a review of the framework had to commence no later than July 25, 2006. In 2007, the Commission proposed a new review of its provisions. The Third Telecoms Legislative Package came into effect in November 2009. Part of it amended the ePrivacy Directive, giving birth to its third chronological version within a period of twelve years since its release.

First, it should be noted that the release of sector-specific regulations in the data protection field was welcomed back in 1997, and was indeed suggested as the preferred way forward for effective data protection regulation. Ever since the Data Protection Directive was released, it was thought that the text only set the general principles for data protection, which would subsequently become concrete to the needs of each data protection sector through specialized legislation.[41] Telecommunications, being at the forefront of the Community legislators' priority list during the 1990s, constituted an obvious place to start implementing this policy.

A second point of equal importance refers to the periodicity of legislative reviews. Because telecommunications are a sector constantly in flux, a statutory provision has been introduced as to the periodical review of the regulatory framework.[42] This statutory obligation has been closely observed so far, and is indeed necessary within the current telecommunications and Internet field. This technically-imposed periodicity, however, also applies to the ePrivacy Directive, as an integral part of the various Telecoms Legislative Packages.

---

40. Directive 2002/21/EC, of the European Parliament and of the Council of 7 March 2002 on a Common Regulatory Framework for Electronic Communications Networks and Services, 2002 O.J. (L 108) 33 (hereinafter "Framework Directive"); Directive 2002/19/EC, of the European Parliament and of the Council of 7 March 2002 on Access to, and Interconnection of, Electronic Communications Networks and Associated Facilities, 2002 O.J. (L 108) 7 (hereinafter "Access Directive"); Directive 2002/20/EC, of the European Parliament and of the Council of 7 March 2002 on the Authorisation of Electronic Communications Networks and Services, 2002 O.J. (L 108) 21 (hereinafter "Authorisation Directive"); Directive 2002/77/EC, of 16 September 2002 on Competition in the Markets for Electronic Communications Services, 202 O.J. (L 249) 21 (hereinafter "Competition in Markets Directive"); Regulation (EC) No 2887/2000, of the European Parliament and of the Council of 18 December 2000 on Unbundled Access to the Local Loop, 2000 O.J. (L 336) 4 (hereinafter "Unbundled Access Regulation"); Directive on Privacy and Electronic Communications, which constitutes, amended as per the recent Telecoms Reform Package, the current ePrivacy Directive.

41. *See* Data Protection Directive; DAMMANN & SIMITIS, *supra* note 9, at 65.

42. *See* Framework Directive.

4. THE 1997 ePRIVACY DIRECTIVE (1997/66/EC)

All EU data protection Directives regulating the telecommunications sector were specifically released in order to closely track technological developments. This, apart from their substance, also affected their naming. Accordingly, the first such Directive chronologically, Directive 1997/66/EC, was named the "Telecoms Data Protection Directive." The 1997 ePrivacy Directive was expressly intended to "particularize and complement" the Data Protection Directive, already in effect since 1995, with the aim of warranting both the right to privacy with respect to the processing of personal data in the telecommunications sector and the free movement of data, equipment, and services within the EU.[43] Its technical, sector-specific character was ensured through a series of provisions, for instance, on traffic and billing data, itemized billing, presentation and restriction of calling and connected line identification, automatic call forwarding, directories of subscribers, or technical features and standardisation.[44] It also chose to apply to legal persons as well, a departure from the natural-persons only limitation of the Data Protection Directive. The individual right to data protection was strengthened and "customized" to the needs of telecommunications-related processing though a series of provisions on security and confidentiality of the communications (in its Articles 4 and 5, respectively). Perhaps interestingly, Article 12 of the 1997 ePrivacy Directive included a provision on "unsolicited calls," protecting consumers from unsolicited communications that seem to have attracted the lawmakers' attention as early as 1997.[45]

5. THE 2002 ePRIVACY DIRECTIVE (2002/58/EC)

The 1997 ePrivacy Directive had been accused of being outdated at the moment of its introduction. It had been drawn up in the first half of the 1990s and it applied only to the "telecommunications" sector, whereas by 1997 the Internet and electronic communications had already emerged forcefully.[46] The 1999 Communications Review suggested

---

43. Processing Directive, arts. 1 and 2; *see also* LLOYD, *supra* note 9 (discussing its lawmaking passage).

44. *See* Processing Directive, arts. 6, 7, 8, 10, 11, and 13.

45. "The use of automated calling systems without human intervention (automatic calling machine) or facsimile machines (fax) for the purposes of direct marketing may only be allowed in respect of subscribers who have given their prior consent,." 1997 ePrivacy Directive, art. 12.

46. In this context, the Commission's 1999 Communications Review noted that:

> The terminology used in the Telecoms Data Protection Directive, which was proposed in 1990, is appropriate for traditional fixed telephony services but less so for new services which have now become available and affordable for a wide public. This creates ambiguities and has led in practice to divergence in national transposition of the Directive. To ensure a consistent application of data protection princi-

an overall review of the First Telecoms Legislative Package "in the light of technical and market developments and changes in user demand." The proposed Second Telecoms Legislative Package would

> address the emerging shortcomings of the current framework for telecommunications, and take into account the market and technological developments. . .seek to reinforce competition in all market segments, particularly at the local level. . .be designed to cater for new, dynamic and largely unpredictable markets with many more players than today. . .ensure a light regulatory approach for new service markets, while ensuring that dominant players do not abuse their market power.[47]

A period of consultation followed. In 2002 the Second Telecoms Legislative Package ("Second Package") was finally adopted.[48] However, not all Directives comprising the Package were adopted simultaneously. Indicative of the controversial nature of many of the issues involved and the intensive negotiations into which it was entangled, the data protection instrument was adopted several months after the other Directives were introduced (July and February 2002, respectively), a delay that affected its transposition into national EU legislations (by October, rather than by July of the same year).

An important factor that held a central role during negotiations for the release of the Second Package, including the ePrivacy Directive, refers to the fact that, by 2002, telecommunications became a multi-billion market within the EU. The opening up of the telecommunications market, initiated in the 1990s, proved to be a success story for the EU. Within only ten years companies worth billions were created (of course, due account ought to be given to the emergence of mobile telephony and the Internet as well). This development greatly affected the release of the Second (and Third) Telecoms Legislative Package. In practice, even a minor change in legislation could mean millions of expenses for the players involved. On the other hand, the same minor change could ultimately affect the everyday life of every EU individual. In this context, negotiations were hard and included the ePrivacy Directive as an integral part of any Telecoms Legislative Package.

> ples to public telecommunications services and network throughout the EU, the Commission proposes to update and clarify the Directive taking account of technological developments converging markets.

The 1999 Communications Review; see also LLOYD, *supra* note 9, at 161; *see also* Frederic Debussere, *The EU e-Privacy Directive: A Monstrous Attempt to Starve the Cookie Monster?*, 13 INT'L J. INFO. TECH. 70, 92 (2005), *available at* https://www.law.kuleuven.be/icri/publications/657FredericDebussereCookies.pdf.

47. *See The 1999 Communications Review*, *supra* note 37, at 539.

48. The Second Telecoms Legislative Package was mainly comprised of the Framework Directive, Access Directive, Authorisation Directive, Universal Service Directive, Directive on Privacy and Electronic Communications, Competition in the Markets Directive, and Unbundled Access Regulation.

The 2002 ePrivacy Directive expressly replaced the 1997 ePrivacy Directive.[49] With regard to its provisions, the structure of the 2002 ePrivacy Directive broadly followed that of its predecessor: special articles were devoted to security and confidentiality of the communications, traffic data, itemized billing, calling line identification, directories of subscribers, unsolicited communications, and technical features and standardization.[50] The 2002 ePrivacy Directive provisions equally aimed to particularize and complement those of the Data Protection Directive.[51] In addition, they applied by now to "the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks in the Community" (Article 3.1), explicitly abandoning "telecommunications" and thus breaking up with the past, at least from a terminology point of view.[52]

A crucial distinction that remains at the epicenter of disputes (see *infra*, Section 12) refers to the actual recipients of the ePrivacy Directive. In an already increasingly convergent technological environment, whereby voice and data services are provided both by traditional telecommunications players and Internet businesses, it is important to note that the 2002 ePrivacy Directive was only addressed to the telecommunications players.[53] Therefore, "data controllers" in the 2002 ePrivacy Di-

49. Directive on Privacy and Electronic Communications, recital 4.

50. *See* 2002 ePrivacy Directive, arts. 4, 5, 6, 7, 12, 13, and 14.

51. However, its actual wording did cause some disputes in legal theory as to whether it actually pertains to "any" data or only to "personal" data, ultimately building (exclusively) upon the Data Protection Directive premises, or perhaps occasionally moving away from them. A number of arguments point to a certain degree of non-complete overlap of scopes between the two Directives, such as the fact that the ePrivacy Directive refers to "privacy" and not "data protection" in its title, the fact that the term "personal data" is carefully avoided in its text with regard to "traffic data" or "localisation data," or the fact that the term "information" (rather than "personal data") is the preferred term in its text. Nevertheless, it should be noted that the mainstream perception, as expressed by the Article 29 Working Party, is that, except for the provisions with regard to legal persons, the scope of the two Directives overlap, with the Data Protection Directive setting the general rules that the ePrivacy Directive makes specific to the electronic communications sector. In addition, with regard to challenges to the "personal data" definition in the amended ePrivacy Directive context, *see* Yves Poullet, *About the E-Privacy Directive: Towards a Third Generation of Data Protection Legislation?*, *in* DATA PROTECTION IN A PROFILED WORLD 3, 9 (Serge Gutwirth et al. eds., 2010).

52. Directive on Privacy and Electronic Communications.

53. Directive 2000/31/EC, of the European Parliament and of the Council of 8 June 2000 on Certain Legal Aspects of Information Society Services, in Particular Electronic Commerce, in the Internal Market, art. 2, 2000 O.J. L 178) 28 (hereinafter "E-Commerce Directive").

> An Electronic communications service means a service normally provided for remuneration which consists wholly or mainly in the conveyance of signals on electronic communications networks, including telecommunications services and transmission services in networks used for broadcasting, but exclude services providing, or exercising editorial control over, content transmitted using electronic

rective were only "telecommunications companies and providers of Internet access"[54] and not Information Society Service Providers[55] (all businesses over the Internet). In a simple example as to the limitations that were soon to be witnessed of this approach, Skype would not be regulated by the ePrivacy Directive, because it provides voice services over the Internet and not over cable networks.

Additionally, the 2002 ePrivacy Directive placed security obligations upon service providers in the form of technical and organizational measures and informing users and subscribers;[56] the latter became of central importance while negotiating its amendment in the Third Telecoms Legislative Package.

Data protection safeguards included various individual rights, including the right to receive non-itemized bills, to opt-out to being included in a directory, or to block caller identification. Unsolicited communications (spam) continued to constitute an issue of concern: the 2002 ePrivacy Directive introduced an opt-in system whereby the use of e-communication media, such as email and Short Message Service ("SMS") text message for the purposes of direct marketing, was only allowed towards subscribers who had given their prior consent, except where the electronic contacts were obtained directly from the customer in the context of a sale of a product or service for similar products and services.[57] Individuals also had the right to object to such processing of their data (i.e. opt-out).[58]

By the time the 2002 ePrivacy Directive was released, the Article 29 Working Party was already established and been quite active in its insti-

---

communications networks and services; it does not include information society services, as defined in Article 1 of Directive 98/34/EC, which do not consist wholly or mainly in the conveyance of signals on electronic communications networks.

Id.

54. *See Second Opinion of the European Data Protection Supervisor on the Review of Directive 2002/58/EC Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector,* para. 22, 2009 O.J. (C 128) 28 (hereinafter "*Second Opinion*").

55. As defined in the E-Commerce Directive; Directive 98/34/EC of the European Parliament and of the Council of 22 June 1998 Laying Down a Procedure for the Provision of Information in the Field of Technical Standards and Regulations and of Rules on Information Society Services, art. 1, 1998 O.J. (L 24) 37 ("hereinafter Procedure Directive").

56. Service providers "must take appropriate technical and organisational measures to safeguard the security of their services, if necessary in conjunction with the network provider and having in regard the state of the art and the cost of their implementation." Directive on Privacy and Electronic Communications. In case of a particular risk of a breach of the security of the network, the service provider must inform the subscribers of such risk and, where the risk lies outside the scope of the measures to be taken by the service provider, of any possible remedies, including an indication of the likely costs involved. *Id.* at art. 4.2.

57. *See* 2002 ePrivacy Directive, art. 13.

58. *Id.*

tutional role[59] of commenting on developments in the electronic communications sector from a data protection perspective.[60] The Article 29 Working Party thus became an increasingly active, and central player while the Third Telecoms Legislative Package (and through it, the second version of the e-Privacy Directive) was being formulated.

6. THE LAW ENFORCEMENT ePRIVACY EXCEPTION CREATED BY THE 2006 DATA RETENTION DIRECTIVE (2006/24/EC)

As per the pre-Lisbon Treaty Pillar system, the ePrivacy Directive could only regulate commercial communications. Even then, it also had to comply with restrictions of its legal basis, the Data Protection Directive. Therefore, public security, defense, and criminal law-related processing were exempted altogether.[61] The post-9/11 climate, however,[62] did not leave the European telecommunications sector unaffected. Building upon space for national law derogations permitted by the 2002 ePrivacy Directive (in its Article 15.1), certain Member States began retaining electronic communications data for purposes of national security. This development ultimately led to the introduction of a relevant Directive, the 2006 Data Retention Directive.[63]

---

59. *See* Processing Directive, art. 14.3.

60. *See* Article 29 Data Protection Working Party, Recommendation 3/97, Anonymity on the Internet, XV D/5022/97 final, WP 6, Dec. 3, 1997, *available at* http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/1997/wp6_en.pdf; Article 29 Data Protection Working Group, Recommendation 1/99 on Invisible and Automatic Processing of Personal Data on the Internet Performed by Software and Hardware, 5093/98/EN/final, WP17, Feb. 23, 1999, *available at* http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/1999/wp17en.pdf;. Article 29 Data Protection Working Group, Recommendation 3/99 on the Preservation of Traffic Data by Internet Service Providers for law Enforcement Purposes, 5085/99/EN/final, WP 25, Sep. 7, 1999, *available at* http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/1999/wp25en.pdf; Article 29 Data Protection Working Group, Opinion 2/2000 Concerning the General Review of the Telecommunications Legal Framework, 5009/00/EN, WP 29, Feb. 3, 2000, *available at* http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2000/wp29.en.pdf.

61. Data Protection Directive, art. 3; Directive on Privacy and Electronic Communications, arts. 1 and 3.

62. On the effect of these developments to EU data protection *see* Paul de Hert & 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 REV. 403-414 (2009).

63. 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 Service or of Public Communications Networks and *amending* Directive 2002/58/EC, 2006 O.J. (L 105) 54 (hereinafter "Data Retention Directive"); *see also* Eleni Kosta & Peggy Valcke, *Retaining the Data Retention Directive*, 22 COMPUTER L. & SECURITY REV. 370, 340 (2006).

The Data Retention Directive partially amended the 2002 ePrivacy Directive, building upon the assumption that data relating to the use of electronic communications are particularly important in the prevention, investigation, detection, and prosecution of criminal offenses.[64] In effect, it requires that electronic communications data, meaning data that are generated or processed by providers of electronic communications services while providing their services, are retained for future use in the state security context. The retention period may vary from between six months to two years.

An analysis of the Data Retention Directive lies outside the scope of this paper. Here it is enough to note that until late-2010 several Member States – Austria, Sweden, and Greece – were reluctant to introduce it into their national legislation; on the other hand, some of the law-abiding Member States met with public outrage when introducing the new instrument at a national level. Several Member States' Constitutional Courts also ruled against Data Retention Directive.[65] Indeed, the Data Retention Directive was, and still is, lamented as a compromise of data protection for security purposes; at the time of its first assessment doubts were expressed as to its usefulness and effectiveness of its provisions.[66] However, for as long as the Data Retention Directive remains in effect it continues to be an integral part of the EU data protection telecommunications legislative framework.[67]

7. THE PREPARATORY PHASE LEADING UP TO 2009 ePRIVACY DIRECTIVE

As per the statutory requirement to periodically review any Telecoms Legislative Package in effect,[68] in 2005 the review of the "functioning" of the Second Package needed to begin, executed by the Commis-

64. *See* Data Retention Directive, recital 7.

65. *See* Bundesverfassungsgericht (BVerfG) (Federal Constitutional Court) Mar. 2, 2010, 1 BvR 256/08, 2010, (Ger.); Romanian Constitutional Court, Oct. 8, 2009, decision no. 1258, Romanian Official Monitor no. 789 (Nov. 23, 2009), *available at* http://www.legi-Internet.ro/fileadmin/editor_folder/pdf/decision-constitutional-court-romania-data-retention.pdf (unofficial translation); *see also* Supreme Court of Cyprus, 65/2009, Feb. 1, 2011, *available at* http://www.supremecourt.gov.cy/Judicial/SC.nsf/All/5B67A764B86AA78EC22578 2F004F6D28/$file/65-09.pdf (Greek).

66. *See* Article 29 Data Protection Working Party, Report 01/2010 on the Second Joint Enforcement Action: Compliance at National Level of Telecom Providers and ISPs with the Obligations Required from National Traffic Data Retention Legislation on the Legal Basis of Articles 6 and 9 of the e-Privacy Directive and the Data Retention Directive 2006/24/EC Amending the e-Privacy Directive., 00068/10/EN, WP 172, July 13, 2010, *available at* http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp172_en.pdf.

67. *See European Commission, Evaluation Report on the Data Retention Directive*, COM (2011) 225 final (Apr. 18, 2011).

68. *See* Framework Directive, art. 25.

sion and reported to the European Parliament and to the Council of the European Union ("Council"). In the end of 2004, the Commission carried out the mandate and announced the launching of the review when announcing its 2010 initiative.[69] In 2005 the Commission launched a public consultation on the review of the Telecoms Package.

In 2006 the Commission presented a report to the European Parliament and the Council on the functioning of the regulatory framework.[70] An underlying idea in the report was that there was room for improvement in the field of consumer protection and security to keep pace with technological developments and remain effective. The Council, from its part, defined the "future challenges for the electronic communications regulatory framework."[71] A new consultation was launched by the Commission in June 2006.[72] On the basis of its results the Commission adopted a Proposal for a Directive in November 2007.[73]

In its first reading, on September 24, 2008, the European Parliament adopted amendments to the Commission's proposal[74] that were

---

69. *See Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee on the Regions, Challenges for the European Information Society Beyond 2005*, COM (2004) 757 final (Nov. 19, 2004).

70. *Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions on the Review of the EU Regulatory Framework for Electronic Communications Networks and Services*, SEC (2006) 816 COM (2006) 334 final (Jun. 29, 2006).

71. *See* Press Release, Council of the European Union, Transport, Telecommunications and Energy 27, 10042/06 (Presse 167), *available at* http://www.consilium.europa.eu/ueDocs/cms_Data/docs/pressData/en/trans/89954.pdf.

72. *See id.*

73. *Proposal for a Directive of the European Parliament and of the Council Amending Directive 2002/22/EC on Universal Service and Users' Rights Relating to the Electronic Communications Networks, Directive 2002/58 EC Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector and Regulation (EC) No 2006/2004 on Consumer Protection Cooperation,* COM (2007) 698 final (Nov. 13, 2007) (hereinafter "*2007 Proposal*").

74. *See* European Parliament Legislative Resolution of 24 September 2008 on the Proposal for a Directive of the European Parliament and of the Council Amending Directive 2002/22/EC on Universal Service and Users Rights Relating to Electronic Communications Networks, Directive 2002/58/EC Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector, and Regulation (EC) No. 2006/2004 on Consumer Protection Cooperation (COM(2007)0698 – C6-0420/2007 – 2007/0248(COD)), 2010 O.J. (C 8E) 359; European Parliament Legislative Resolution of 24 September 2008 on the Proposal for a Directive of the European Parliament and of the Council Amending Directive 2002/21/EC on a Common Regulatory Framework for Electronic Communications Networks and Services, Directive 2002/19/EC on Access to, and Interconnection of, Electronic Communications Networks and Associated Facilities, and Directive 2002/20/EC on the Authorisation of Electronic Communications Networks and Services (COM(2007)0697 – C6-0427/2007 – 2007/0247(COD), 2010 O.J. (C 8E) 291; *see also*

commented back in November 2008 by the European Commission.[75] On November 27, 2008 the Council reached a political agreement. In its second reading, on May 5, 2009, the European Parliament amended the Proposal, in effect deciding not to turn the French Three Strikes Law initiative into European law. The Council disagreed and the conciliation process began. The elections for a new Parliament in the summer of 2009 further delayed progress on the proposal text; finally, a compromise was reached on November 25, 2009, and the Third Telecoms Legislative Package ("Third Package") came into effect on December 18, 2009, two years after the Commission's initial draft proposal was released. In effect, the Third Package comprises two Directives[76] and one Regulation.[77]

8. THE MAIN CHALLENGES AND CONTROVERSIES OF THE 2009 ePRIVACY DIRECTIVE AT THE TIME OF ITS VOTE AND DURING ITS IMPLEMENTATION PERIOD

The regulatory passage towards the Third Package, and in particular towards the amended ePrivacy Directive, was neither swift nor uncontested. Indeed, during the lawmaking process all bodies involved, whether institutional (the Commission, the Council, the Parliament, the Article 29 Working Party, the EDPS) or not, and all stakeholders (the industry, non-governmental organizations ("NGOs"), etc.) took active part in negotiations; the result, as will be later demonstrated, could be seen as a compromise between the relevant conflicting interests.

An initial distinction needs to be repeated here with regard to the Commission. As already noted, it is the DG for Information Society and Media[78] that is involved in drafting the ePrivacy Directive and not the

---

ePrivacy Directive Debated in the EP's Civil Liberties Committee, EDRI-GRAM, Number 6.13, (July 2, 2008), http://www.edri.org/edrigram/number66.13/e-privacy-review-ep.

75. *European Commission, Amended Proposal for a Directive of the European Parliament and of the Council Amending Directive 2002/22/EC on Universal Service and Users' Rights Relating to Electronic Communications Networks, Directive 2002/58/EC Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sectors, and Regulation (EC) No 2006/2004 on Consumer Protection Cooperation,* COM (2008) 723 final (Nov. 6, 2008).

76. 2009 Amending Directive; Directive 2009/140/EC of the European Parliament and of the Council of 25 November 2009 *amending* Directives 2002/21/EC on a Common Regulatory Framework for Electronic Communications Networks and Services, 2002/19/EC on Access to, and Interconnection of, Electronic Communications Networks and Associated Facilities, and 2002/20/EC on the Authorisation of Electronic Communications Networks and Services, O.J. (L 337) 37 (hereinafter "Directive 2009/140/EC").

77. Regulation (EC) No 1211/2009, of the European Parliament and of the Council of 25 November 2009 Establishing the Body of European Regulators for Electronic Communications (BEREC) and the Office, O.J. (L 337) 1.

78. At the time, the Commissioner was Viviane Reding; in the second Barrosso Commission, in 2010, she changed roles, becoming Commissioner for Justice, Fundamental Rights and Citizenship.

DG for Justice, who was normally authorized to regulate data protection matters, at least in the pre-Lisbon environment.[79] This change of DGs has its own meaning while reaching compromise among data protection proponents and stakeholders. The Article 29 Working Party followed the process closely, issuing altogether three Opinions, following the stages of the lawmaking process (and the different Directive drafts): Opinions 8/2006, 2/2008, and 1/2009. The EDPS, for its part, issued a First Opinion in 2008[80] and a Second Opinion in 2009,[81] following drafts and discussions on the Directive draft.

The broader telecommunications picture also should not be missed; data protection, as represented through the ePrivacy Directive, constituted only one of the priorities of the amendment process. Indeed, it could even be maintained that stronger data protection had not merely been an end to itself during the Telecoms Reform lawmaking process, but rather a means to the broader end of ensuring a higher level of public trust, thus strengthening the role of telecommunications in an open and competitive market.[82] For its part, the industry, already a powerful multi-billion dollar business within the EU, took active part in the negotiations: any legislative change, regardless of size, could mean substantial investments in time and money or the gaining or loss of a competitive advantage.

NGOs, on the other hand, also took active part, if not directly, in the negotiations;[83] the fact that, by 2008, electronic communications were found at the basis of a social, rather than a purely technological, phenomenon meant that the everyday lives of virtually every EU citizen would be affected by the outcome.

Ever since the first drafts of the Third Package in 2007 were released, convergence was the main trend in the telecommunications sec-

79. On the change of Directorates within the EU institutions and its effect on data protection, *see* de Hert, *supra* note 17, at 163.

80. *Opinion of the European Data Protection Supervisor on the Proposal for a Directive of the European Parliament and of the Council Amending, Among Others, Directive 2002/58/EC Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector,* 2008 O.J. (C 181) 1 (hereinafter "*First Opinion*").

81. *Second Opinion,* para. 22.

82. *See Commission Proposal for a Directive of the European Parliament and of the Council Amending Directive 2002/21/EC on a Common Regulatory Framework for Electronic Communications Networks and Services, 2002/19/EC on Access to, and Interconnection of, Electronic Communications Networks and Services, and 2002/20/EC on the Authorisation of Electronic Communications Networks and Services,* COM (2007) 697 final (Nov. 13, 2007) (hereinafter "*Common Regulatory Framework Proposal*").

83. *See* Erik Josefsson, *Seminar the Telecoms Package and Network Filtering*, EUROPEAN DIGITAL RIGHTS, Aug. 27, 2008, *available at* http://www.edri.org/edrigram/number6.16/telecoms-package-seminar.

tor.[84] This trend continued to be very much relevant in 2009, when the Third Package was finally adopted. Increasingly, telecommunications ceased to mean only the transmission of voice, and even some data, over dedicated networks. Instead the Internet, mostly through Voice over Internet Protocol ("VoIP"), assumed a complimentary or even substitution role.

In this context, an important challenge for the Third Package was the fact that service providers could no longer be traced as easily as in the past. Back in the 1980s, when the First Telecoms Legislative Package aimed at opening up the market,[85] service providers were easy to spot: essentially, each Member State had one, a local monopoly or incumbent provider. Mobile telephony was not yet an issue. The Second Package saw the establishment of mobile telephone and the rising (and falling) of alternative fixed line telephony providers across Europe. Still, until that time, the Second Package was essentially addressed to a handful of service providers, easily identifiable. On the contrary, the Third Package coincided with the convergence of Internet and telecommunications (both mobile and fixed line) technologies. Increasingly, service providers are difficult to distinguish, as Internet providers also provide voice and content services, while traditional telephony providers enter the Internet market. In other words, the amended ePrivacy Directive is not expected to have an easy time distinguishing its recipients, at least from the data processor point-of-view.[86]

In the meantime, however, implementation difficulties for the amended ePrivacy Directive, at least with regard to its scope, have, perhaps unexpectedly, come from the proliferation of mobile phone applications ("apps"). Because the ePrivacy Directive, even in its latest wording, is intended to regulate "publicly available electronic communications services,"[87] and, by 2011, when it is supposed to come into effect in Member States' legislation, it can be argued that "app stores" (for instance, Apple's iTunes, Microsoft's Marketplace, and Google's Android Play) do not fall under this category, it could be argued that the Directive's provisions do not apply to these operators.

Internet copyright piracy also came to be relevant while preparing the Third Package, an unforeseen development until that time. Although the relevant analysis will follow in Section 13, it is enough to highlight the by now well-known problem: increasing volumes of unlawful exchanges of copyright-protected material over the Internet threaten the

84. *See Telecoms and the Internet: The Meaning of Free Speech*, ECONOMIST (Sep. 15, 2005), http://www.economist.com/node/4400704.

85. *See* Section 3.

86. *See also infra*, Section 12.

87. *See* Directive on Privacy and Electronic Communications, art. 2(d).

very existence of the Content Industry. Having armed itself with favorable case law,[88] the Content Industry has entered a worldwide campaign to control unlawful file exchanges among users. The ISPs, as access providers and thus "gatekeepers," are an obvious target for petitions and lobbying towards increased policing of their clients.

Another issue that was discussed during the lawmaking process of the Third Package, with only partial relevance to the ePrivacy Directive, refers to network neutrality. Network neutrality means that no restrictions are placed by ISPs or anybody else on content, sites, platforms, or equipment.[89] The term was allegedly first used in the United States by telecommunications companies who saw Internet companies thrive, in their eyes at least, at their expense; because the telecommunications infrastructure is built at great cost by the telecommunications companies, Internet companies may start providing services without any substantial investment. The fair solution for Internet companies or users – according to telecommunications companies – would be to pay to the telecommunications companies something extra for better (speedier) access services. However, this would create a multi-level Internet, whereby some users and Internet websites would inevitably be left behind. The Telecoms Reform Package found itself temporarily at the epicentre of relevant international discussions, with intensive lobbying from both sides of the argument.[90]

As evidenced above, a number of issues and players held various roles while preparing the EU Third Telecoms Legislative Package. The ePrivacy Directive, as its integral part, was unavoidably dragged into the relevant disputes, and was frequently used as a negotiations tool, despite the fact that the above issues and the various agendas of each of the participating bodies were not always related to the its subject matter; that is, to data protection.

The amended ePrivacy Directive was supposed to be implemented into Member State national laws by May 25, 2011.[91] However, only a

88. *See* MGM Studios, Inc. v. Grokster, Ltd., 545 U.S. 913 (2005); Svea Horvatts [HoVR] [Svea Court of Appeals] 2010-11-26 B4041-09 (Swed.) (case of Pirate Bay in Sweden).

89. On the issue of "network neutrality" *see* Tim Wu, *Network Neutrality, Broadband Discrimination*, 2 J. TELECOMM. & HIGH TECH. L. 141 (2003), *available at* SSRN: http://ssrn.com/abstract=388863 or doi:10.2139/ssrn.388863.

90. *See also European Commission Communication, The Open Internet and Net Neutrality in Europe*, COM (2011) 222 final, (Apr. 19, 2011). However, the relevant discussion remains open years after the Third Telecoms Legislative Package release – see for instance, the Commission's 'Open Internet and neutrality' consultation in early 2012, at http://ec.europa.eu/information_society/policy/ecomm/current-topics/net_neutrality/index_en.htm.

91. *See* 2009 Amending Directive, art. 4.

handful of EU Member State seems to have observed this deadline.[92] In fact, almost a year later still there exist no information in the Commission's official website on the status of national implementation,[93] a fact probably meaning that Member States have been hesitant in fulfilling their duties.[94] The release, in early 2012, of the draft Commission's proposals for the reform of the general EU data protection framework[95] are expected to further delay Member State implementation of the ePrivacy Directive, because most Member States would, understandably, prefer not to duplicate efforts.

This entanglement into complex negotiations is perhaps unavoidable for the ePrivacy Directive, given the broad character of the amendment process brought forward by this, the third review of the EU Telecoms Legislative Package, in addition to those that will, periodically, follow. The data protection outcome is, and shall continue to be, affected by technological and financial considerations and developments not entirely connected to it. Therefore, it remains unclear whether the annexing of data protection (in particular, the ePrivacy Directive) to a comprehensive, periodical telecoms regulatory review ultimately helps its purposes. The breadth of issues discussed and the stakes during the lawmaking process of such a central piece of legislation in contemporary societies perhaps changes the focus from individual data protection to other considerations.

9. NEW PROVISIONS ON INTEGRITY OF ELECTRONIC COMMUNICATIONS SYSTEMS: ARTICLE 4 OF THE ePRIVACY DIRECTIVE

The security of the processing is a fundamental data protection principle, expressly established in the text of the Data Protection Directive:

---

92. For example, the United Kingdom's amended Privacy and Electronic Communications Regulations, which became effective May 26, 2011. According to the Information Commissioner's Office, "[m]ost of the Regulations are still the same and our existing guidance still applies. The major changes relate to cookies, the need for public electronic communications service providers to report personal data breaches, and the powers the Information Commissioner has to enforce these regulations. *What do I Need to Know About the Amended Regulation,* INFORMATION COMMISSIONER'S OFFICE (May 26, 2011), http://www.ico.gov.uk/for_organisations/privacy_and_electronic_communications/new_regulations.aspx.

93. *Available at* http://ec.europa.eu/information_society/policy/ecomm/eu-rules/index_en.htm.

94. It should be noted, however, that neither has the Commission initiated any court proceedings against Member States for this reason either. *Infringement of EU Law*, EUROPEAN COMMISSION (Aug. 17, 2011), http://ec.europa.eu/information_society/policy/ecomm/implementation_enforcement/infringement/index_en.htm).

95. *See* Section 2.

> Member States shall provide that the controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing. Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.[96]

As such, the principle is set in broad terms, covering each and every kind of personal data processing. While the security of the processing is a self-evident and fundamental general data protection principle that hardly requires further elaboration, its more interesting part refers to its proportionality criterion: according to the Data Protection Directive wording, "measures shall ensure a level of security appropriate to the risks."[97] The proportionality[98] of security measures to the processing risks itself, in a way, warrants the viability of the principle of the security of processing; without it, its technical requirements would vanish in endless impractical theoretical exercises on network security regardless of the value of the material at stake (personal information).

Telecommunications networks and services, undergoing continuous technical changes and always ready to try new business models, are prone to security attacks or data losses. The security of processing principle thus constitutes a central point of the ePrivacy Directive: its aim is, first and foremost, to provide concrete instructions to service providers as to the measures they need to implement in their systems. It also aims at giving some guidance[99] for striking the balance[100] between security measures and risks, as required by the above proportionality criterion.

The ePrivacy Directive addressed the issue of system security even

---

96. Data Protection Directive, art. 17.1; *see also* DAMMANN & SIMITIS, *supra* note 9, at 222ff.

97. *See* Data Protection Directive, art. 17.1.

98. On the principle of proportionality for EU data protection, *see* Christopher Kuner, *Proportionality in European Data Protection Law And Its Importance for Data Processing by Companies*, 7 PRIVACY & SECURITY L. REP. 1615, 1645 (2008), *available at* http://www.hunton.com/files/Publication145a5e73-17d6-47c0-9fcc-0b45de6575fd/Presentation/PublicationAttachment/da68f827-db96-4b8c-b4ef-0437e358282a/Kuner_Proportionality_in_EU_DataProtectionLaw.pdf; THE BUREAU OF NATIONAL AFFAIRS (BNA), http://bna.com/ (last visited Dec. 12, 2011); Lee A. Bygrave & Dag Wiese Schartum, *Consent, Proportionality and Collective Power, in* REINVENTING DATA PROTECTION?, 57ff. (Serge Gutwirth et al. eds. 2009).

99. The exact point of balance is ultimately for the courts to decide.

100. Not always an easy task; *see* Poullet, *supra* note 51, at 25 (with specific reference and analysis of the 27 February 2008 German Constitutional Court decision (BVerG, 1BvR 370/07) on the intrusion into terminal equipments by law enforcement authorities (with further bibliography).

in its prior version.[101] Its amendment, however, under the Telecoms Reform Package was profound.[102] Other than a change in title, a new paragraph was also inserted:

> 1a. Without prejudice to [the Data Protection Directive], the measures referred to in paragraph 1 shall at least: - ensure that personal data can be accessed only by authorised personnel for legally authorized purposes, - protect personal data stored or transmitted against accidental or unlawful destruction, accidental loss or alteration, and unauthorised or unlawful storage, processing, access or disclosure, and - ensure the implementation of a security policy with respect to the processing of personal data. Relevant national authorities shall be able to audit the measures taken by providers of publicly available electronic communication services and to issue recommendations about best practices concerning the level of security which those measures should achieve.[103]

Therefore, with regard to the proportionality criterion, the amended ePrivacy Directive requires that any service provider ought to at least limit access to the data to authorized personnel only, to implement hardware and software security measures, and to write down and implement a security policy for its processing of personal data.[104] Going forward, all items in the list should constitute the minimum basis for the provision of telecommunication services in the EU.

The requirement to establish and implement a security policy is a further formal obligation for all providers of publicly available electronic communications services in the EU.[105] Limited guidance is provided as to the exact contents of such a policy; the Directive's Recitals only mention that it "should be established in order to identify vulnerabilities in the system," leading to periodical "monitoring and preventive, corrective and mitigating action."[106] In that sense, the security policy is rather envisaged as an assessment of the integrity of the data processing system and not as a formal notification requirement on the details and particulars of the processing.[107] In other words, the security policy should not be a static document illustrating the processing methodology, but rather a periodical security report on shortcomings of the processing system. Because such policies shall be viewable, controllable, and ultimately used

101. Directive on Privacy and Electronic Communications, art. 4.1.

102. 2009 Amending Directive, art. 4.1 (System integrity-related provisions are also found in the text of the amended Framework Directive); *see* Directive 2009/140/EC (for an analysis on data breach notifications).

103. *See* 2009 Amending Directive, art. 2.

104. *See also id.* at recital 57.

105. *See* ePrivacy Directive, art. 4.1.

106. 2009 Amending Directive, recital 57.

107. That, anyway, is mandatory for the provider, as laid down by Article 12 of the Data Protection Directive.

as evidence against them, if this is the case, this change is expected to substantially affect service providers in the EU.

National Data Protection Authorities shall audit the security policies and the measures taken by service providers. In addition, such authorities may recommend best practices on the level of security those measures should aim at, an indirect call for "soft law" to complement the ePrivacy Directive requirements.[108] The means to achieve this are already in place, in the form of codes of practice – "normes simplifiées" – or other self-regulatory instruments.[109]

Admittedly, the drafting of security policies is a welcome addition to obligations already imposed upon service providers by the general provisions of the Data Protection Directive.[110] However, if the amended Data Protection Directive also forces the drafting of Data Protection Impact Assessments upon data controllers,[111] alleviating at the same time other bureaucratic obligations, the electronic communications sector may be left the only one requiring security policies in addition to all the above – a peculiar uniqueness, perhaps not justified by the risks for individual data protection at stake (if, for instance, compared with other industries such as credit or travel or insurance).

System integrity considerations also include the discussion on traffic data processing by companies providing security services to electronic communications networks or service providers. After prolonged negotiations,[112] this issue is now treated in the Recitals of the ePrivacy Directive.[113] Despite the fact that data protection proponents wished for these provisions to be altogether deleted,[114] their inclusion in the text of the

108. *See* ePrivacy Directive, art. 4.1.

109. *See* PAPAKONSTANTINOU, *supra* note 10.

110. Data Protection Directive. The requirements to limit access to the data to authorized personnel only and to implement hardware and software security measures can be inferred from the Data Protection Directive, Section VIII, Confidentiality and Security of Processing, under the general provisions of Articles 16 and 17.

111. *See European Commission Communication*, *supra* note 30.

112. *See Second Opinion*, para. 73ff.

113. *See* 2009 Amending Directive, recital 53. Recital 53 states:

> The processing of traffic data to the extent strictly necessary for the purposes of ensuring network and information security, i.e. the ability of a network or an information system to resist, at a given level of confidence, accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted data, and the security of the related services offered by, or accessible via, these networks and systems, by providers of security technologies and services when acting as data controllers is subject to Article 7(f) of [the Data Protection Directive. This could, for example, include preventing unauthorised [sic] access to electronic communications networks and malicious code distribution and stopping denial of service' attacks and damage to computer and electronic communication systems.

Id.

114. *See Second Opinion*, para. 86.

ePrivacy Directive need not be a complete data protection disaster.[115] These provisions ask for preventive action by network and services providers when it comes to ensuring the integrity of their systems. Permitting traffic data processing, even against individual consent, in order to ensure system security, a service provider will probably have a hard time explaining to individuals, in an event of a breach, why its security policy and preventive security measures did not highlight the risk or why it ignored an already identified security shortcoming.

10. NEW PROVISIONS ON SPAM, PRIVACY-INTRUSIVE TECHNOLOGIES, COOKIES, AND USER CONSENT: ARTICLES 5.3 AND 13 OF THE ePRIVACY DIRECTIVE

The ePrivacy Directive, essentially being particular to the needs of the telecommunications sector, has to remain updated from a technological point of view. Therefore, it could not avoid entangling itself, with a view to bring them under the general EU data protection standards, with such issues as cookies, spam, spyware, computer viruses, and other contemporary telecommunications phenomena.

This is by no means a development that only occurred in the text of the amended ePrivacy Directive; in its previous version, explicit mention was made to "unsolicited communications."[116] The cases of cookies, spyware, web bugs, and hidden identifiers were also expressly treated.[117] Altogether, the previous versions of the ePrivacy Directive probably succeeded, at their respective time, to demonstrate technological relevance, if not effectiveness.[118]

On the other hand, the limitation in scope of the ePrivacy Directive cannot escape attention; normally, the ePrivacy Directive is addressed only to electronic communications service providers and not to information society service providers. Therefore, all Internet-related (e-commerce) activities are expected to escape its purview. However, there is an attempt to rectify this limitation on a case-specific basis only for this type of processing in the text of the amended ePrivacy Directive.

As far as cookies, spyware,[119] and other privacy-intrusive technologies are concerned, the new Article 5.3 sets that:

> Member States shall ensure that the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber

115. Particularly because, as the EDPS himself admits, such processing is generally "likely to meet the requirements of the Data Protection Directive[.]" *Id.* at para 80.

116. Directive on Privacy and Electronic Communications, paras. 40, 43.

117. *Id.* at paras. 24-25.

118. On technological challenges during the lawmaking process, *see* Poullet, *supra* note 51, at 18.

119. For spyware and computer viruses, *see* 2009 Amending Directive.

> or user concerned has given his or her consent, having been provided with clear and comprehensive information, in accordance with [the Data Protection Directive], inter alia, about the purposes of the processing.

Because the previous version of the ePrivacy Directive only made reference to electronic communication networks, and was thus restricted only to them, the Internet largely remained unregulated. This shortcoming was addressed, as seen above, in the text of the amended Directive, much to data protection proponents' satisfaction.[120]

In regard to the particulars of such individual consent, without prejudice to the strict requirements of the Data Protection Directive,[121] the ePrivacy Directive merely asks for users to be provided with clear and comprehensive information before or at the time of processing of their personal information.[122] This information ought to include the categories listed in the Data Protection Directive, most importantly who the data controller is and how individuals may object.

The means of collecting such users' consent are relatively relaxed: "where it is technically possible and effective," it may include the appropriate settings of a browser or other application.[123] On the other hand, the default settings of an Internet browsing software application, if set to automatically accept cookies, cannot count as lawful consent according to the above requirements. Automatic, pre-set settings hardly count as "clear and comprehensive information" as per the ePrivacy Directive requirement. On the contrary, it would appear that the advisable policy for software developers, in order to comply with its requirements, would be to pre-set their Internet browsing applications to not accept cookies (or to the highest possible privacy-protecting level) unless the user expressly chooses differently; it is such settings only that would qualify as user-friendly methods while "providing information" and "offering the right to refuse."[124] For its part, the industry has highlighted the impracticality of the above solutions ("making consumers consent to every cookie presented to them")[125] and has opted indeed for Internet browser pre-set

120. *See First Opinion.*

121. Data Protection Directive, art. 2 ("'The data subject's consent' shall mean any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed."); *see also* DAMMANN & SIMITIS, *supra* note 9, at 103.

122. *See* 2009 Amending Directive, recital 66.

123. *See id.*

124. *Id*. This issue is ultimately connected to the "privacy by design" discussion. *See also 2007 Proposal*.

125. *See Governments*, *supra* note 7.

settings.[126]

Exemptions that ought, however, to be interpreted narrowly, given the retreat to the provisions on consent of the Data Protection Directive, are allowed. These exemptions are aimed at accommodating the technical need to store or access information temporarily (for instance, caching) for the provision of Internet services. Nevertheless, such exemptions need to be limited only to those cases where this technical storage or access is strictly necessary for the provision of a service that the individual requested.[127]

Spam, not only in its email format, has always raised special attention within EU institutions.[128] However, all attempts to resolve the issue, as everybody knows by now, have spectacularly failed. The amended ePrivacy Directive continues to deal with the still open issues of spam or spyware, bringing institutional and practical improvements in the wording of its previous version, while also attempting to remain relevant from a technological (Internet) perspective.

Spam continues to occupy a full article in the text of the ePrivacy Directive.[129] Amendments include an extension of its scope of protection also to "users," instead of the limited circle of "subscribers" only (as was the case in the past), clarification that the right not to receive spam emails should be made available to individuals free of charge, and linguistic improvements.[130] In addition, spam is recognized as such regardless of its technical platform; SMS, Multimedia Messaging Service ("MMS"), and other similar messages may also qualify as unsolicited communications (perhaps artificially extending the meaning of "electronic mail" to also include these other, non-Internet-related forms of communications).[131]

---

126. *See also* the UK's practical guidance with particular emphasis on "cookies" at *Privacy and Electronic Communications Regulations*, INFORMATION COMMISSIONER'S OFFICE, http://www.ico.gov.uk/for_organisations/privacy_and_electronic_communications.aspx.

127. *See* 2009 Amending Directive, art. 5.3 and recital 66. On the exemption in Article 5.3, *see First Opinion.*

128. For email spam *see generally*, Europe's Information Society, *Unsolicited Communications – Fighting Spam, Commissioner Reding Calls on Member States to Reinforce their Efforts in the Fight Against Spam, Spyware and Malicious Software* (Oct. 8, 2009), *available at* http://ec.europa.eu/information_society/policy/ecomm/todays_framework/privacy_protection/spam/index_en.htm. Provisions with direct or indirect relevance to spam may also be found in basic EU data protection practices (see for instance, Data Protection Directive, art. 14b) and ecommerce legislation. *see also* E-Commerce Directive, art. 7; *see also* Gloria Gonzalez Fuster, et al., *From Unsolicited Communications to Unsolicited Adjustments: Redefining a Key Mechanism for Privacy Protection, in* DATA PROTECTION IN A PROFILED WORLD 105, 107 (Serge Gutwirth et al. eds., 2010).

129. *See* ePrivacy Directive, art. 13.

130. *See* 2009 Amending Directive, art. 2.

131. *See id.* at recital 67.

Perhaps the most important amendment with regard to spam refers to the fact that the ePrivacy Directive substantially enlarged the circle of parties with a right to sue spammers.[132] Now, in addition to any other remedies already in place, Member States shall afford to any affected party the right to bring legal proceedings against spammers in their national courts.[133] This right shall not be limited only to the individuals and organizations directly concerned; consumer organizations and trade unions will also be able to sue spammers.[134] In addition, service providers, particularly email service providers,[135] could also undertake legal action against spammers if they feel that their business interests are in any way hurt by spam practices. Practically, therefore, all parties directly or indirectly involved in a typical spamming activity will be authorized to sue independently of each other.

For service providers especially, the amended ePrivacy Directive advises vigilance. If it is established that their negligence contributed in any way to infringements of national regulations regarding spam, specific penalties may be levied upon them.[136] The justification behind the new obligation is that service providers make substantial investments in order to combat spam and are in a better position than users to detect and identify spammers.[137] The level of vigilance that needs to be demonstrated by service providers in order to avoid such risk is anybody's guess. Again, here, the proportionality criterion discussed above is expected to find application. Ultimately, electronic communications service providers are afforded the option to file lawsuits against spammers, and should consider seriously exercising that option if they do not wish to risk being held as negligent and viewed as indirectly contributing to the continuation of unlawful spamming activities.

Finally, a point to be noted here is the case-specific extension of scope of the ePrivacy Directive. In most of the above cases, although the ePrivacy Directive recipients are electronic communications service providers and not information society service providers, the aforementioned provisions expressly extend their scope to also cover the information society (the Internet). This, apart from being awkward from a lawmaking point of view, demonstrates that the ePrivacy Directive, after

132. On the need to "widen the protection currently granted through the regulation of unsolicited communications via the new notion of 'unsolicited adjustments,'" *see* Fuster, *supra* note 128, at 115.

133. *See* 2009 Amending Directive, art. 13.6.

134. *See First Opinion*, para. 52ff.

135. *See* 2009 Amending Directive. It could be argued, however, that under contemporary Internet conditions, email service providers are equally likely to be Internet service providers and not electronic communications service providers.

136. *See id.* at art. 13.6.

137. *See id.* at recital 68.

telecommunications and the Internet converged in the real world, is suffocating and struggling within its lawful boundaries to provide comprehensive and effective solutions to the new reality.

11. PROVISIONS PROTECTING PUBLIC DIRECTORIES OF SUBSCRIBERS: ARTICLE 12 OF THE ePRIVACY DIRECTIVE

Directories of electronic communications services subscribers[138] are essentially "files" in the sense of general data protection law,[139] and are thus regulated by data protection legislation. However, because of the special conditions under which these databases are formed and placed in the market, directories of electronic communications in the EU transcend legislative borders and are regulated both by basic electronic communications legislation and by the ePrivacy Directive; only the former's provisions were amended in the Telecoms Reform Package.[140]

Telephone directories, for as long as telecommunications were provided in EU Member States by national monopolies through a state incubator, formed a service, against a fee or free of charge, provided by such incubator to its subscribers. After the opening up of the telecommunications market, through the First Telecoms Legislative Package, telephone directories as a service was, by means of a relevant provision in the Legislative Package, taken away from the incubator monopoly and released in the market for anyone to take up and develop commercially.[141] This opening up of the telephone directories market and the creation of a new business model was regulated by Article 25 of the Universal Service Directive.

The Universal Service Directive was amended under the Telecoms Reform Package by the same Directive 2009/136 amending the 2002 ePrivacy Directive. Article 25 is among those amended; nevertheless, paragraph 5, even in its new wording, continues to refer expressly to Ar-

138. In this case, service subscribers only refer to fixed or mobile telephones.

139. Data Protection Directive, art. 2 ("Any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis.").

140. *See* ePrivacy Directive, art. 12.

141. Despite the explicit legislative mention, the same effect – the opening up of the telephone directory market to competition – would probably have been achieved at any event through other means, because such directories are "databases" in the sense of the Database Directive. *See* Directive 96/9/EC, of the European Parliament and of the Council of 11 March 1996 on the Legal Protection of Database, art. 1.2, 1996 O.J. (L 77) 20 (hereinafter "Database Directive'). Additionally, the ECJ, in its British Horseracing decision (Case C-203/02, British Horseracing Board Ltd. V. William Hill Organization Ltd., 2004 E.C.R. 0, 1 C.M.L.R. 15 (2004)) ruled against proprietary rights on the contents of such databases by incubators or, at any event, institutions who helped create this information.

ticle 12 of the ePrivacy Directive regarding data protection issues.[142] For its part, the relevant provisions of the 2002 ePrivacy Directive, including Article 12, were not amended. Hence, notwithstanding the somehow complicated lawmaking mechanism, data protection rights of individuals should normally not be affected by amendments with regard to telephone directories.[143]

12. PERSONAL DATA BREACH NOTIFICATIONS: ARTICLE 4.3 OF THE ePRIVACY DIRECTIVE

One of the most disputed issues during the ePrivacy Directive amendment process referred to security breach notifications.[144] At the same time the Telecoms Reform Package was being discussed, public opinion in several EU Member States was astonished to hear, mostly from journalists and not from the perpetrators themselves, about spectacular losses or compromises of their personal information stored mostly in government systems.[145] Such losses came in varying volumes and formats and, admittedly, telecommunications networks were not always to blame. However, what these losses all had in common was the substantial breach of individual data protection and lack of a formal notification to the individuals concerned in order for them to enact measures to protect themselves after the data breach had occurred. On the other hand, it is obvious that such notifications would incur substantial resources, not to mention the bad publicity, for the organizations

142. 2009 Amending Directive ("Paragraphs 1 to 4 shall apply subject to the requirements of Community legislation on the protection of personal data and privacy and, in particular, Article 12 of [the ePrivacy Directive].").

143. Some data protection interest may be found in Recital 33 of the Universal Service Directive:

> Customers should be informed of their rights with respect to the use of their personal information in subscriber directories and in particular of the purpose or purposes of such directories, as well as their right, free of charge, not to be included in a public subscriber directory, as provided for in [the ePrivacy Directive]. Customers should also be informed of systems which allow information to be included in the directory database but which do not disclose such information to users of directory services.

Id.; 2009 Amending Directive, recital 33.

144. *See* Article 29 Data Protection Working Party, Working Document 01/2011 on the Current EU Personal Data Breach Framework and Recommendations for Future Policy Developments, 00683/11/EN, WP 184 Apr. 5, 2011, *available at* http://ec.europa/eu.justice/policies/privacy/docs/wpdocs/2011/wp184_en.pdf.; *see also* Rosa Barcelo & Peter Traung, *The Emerging European Union Security Breach Legal Framework: The 2002/58 E-Privacy Directive and Beyond*, *in* DATA PROTECTION IN A PROFILED WORLD 77ff (Serge Gutwirth et al. eds., 2010).

145. *See*, *e.g.*, *UK's Families Put on Fraud Alert*, BBC (Nov. 20, 2007), http://news.bbc.co.uk/2/hi/7103566.stm; *Previous Cases of Missing Data*, BBC, (May 25, 2009), http://news.bbc.co.uk/2/hi/uk_news/7449927.stm.

responsible.[146]

The previous version of the ePrivacy Directive took only passing attention of this matter.[147] Things changed dramatically, however, in the amended text,[148] as, per the revised Article 4.3, "in the case of a personal data breach, the provider of publicly available electronic communications services shall, without undue delay, notify the personal data breach to the competent national authority." Apart from the relatively straightforward notification requirement of the "competent national authority" (most likely, the Data Protection Authority), those responsible need also take care that "when the personal data breach is likely to adversely affect the personal data or privacy of a subscriber or individual, the provider shall also notify the subscriber or individual of the breach without undue delay."

Two points need to be immediately noted before analyzing this addition to the ePrivacy Directive any further. The first point is the basic distinction, that the ePrivacy Directive recipients are only electronic communications services providers (ISPs, telecoms operators) and not information service providers (the Internet). The wording of Article 4.3 means that this obligation to notify is placed upon the former only.[149] This point, that was the epicenter of disputes, will be discussed later in more detail.

Second, the term "personal data breach" denotes "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised [sic] disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of a publicly available electronic communications service in the Community."[150] The list of processing acts that may constitute a data breach according to the provisions of the amended ePrivacy Directive is comprehensive; consequently any use of personal data over open telecommunications networks without lawful grounds would fall within its scope.[151] A willful act or omission of the service provider is not a condition. In addition, "per-

146. However, it has been noted that "fear of reputational sanction may lead, notwithstanding the legal mandate, to excessive secrecy about security breaches involving sensitive customer information." Edward J. Janger & Paul M. Schwartz, *Anonymous Disclosure of Security Breaches: Mitigating Harm and Facilitating Coordinated Responses, in* SECURING PRIVACY IN THE INTERNET AGE 221, 224 (Anupam Chandler et al. eds., 2008); *see also* Paul M. Schwartz & Edward J. Janger, *Notification of Data Security* Breaches, 105 MICH. L. REV. 913 (2007).

147. *See* ePrivacy Directive, art 4.2.

148. On the justification for the introduction of a personal data breach notification system, *see First Opinion.*

149. Barcelo & Traung, *supra* note 144, at 86.

150. *See* 2009 Amending Directive, art. 2; *see also* Barcelo & Traung, *supra* note 144, at 89.

151. *See Second Opinion*, para. 18ff.

sonal data" should be perceived in the broadest sense; to this end, explicit mention is made in the Directive's Recitals of IP addresses.[152]

Individuals are therefore to be notified in the event of a data breach, including breach of personal information, which takes place over telecommunications networks, under the condition that such data breach is likely to adversely affect their personal data or privacy. Because personal data breaches, that is, the loss of personal information, almost always adversely affect the right to data protection or privacy of individuals, notifications should constitute the norm.[153] However, the amended ePrivacy Directive clarifies that "a breach should be considered as adversely affecting the data or privacy of a subscriber or individual where it could result in, for example, identity theft or fraud, physical harm, significant humiliation or damage to reputation in connection with the provision of publicly available communications services in the Community."[154] This list enumerates means by which data loss could negatively affect individuals. Consequently, all personal data breaches should be notified to the individuals concerned.

The recipients of these notifications are subscribers and users alike; the amended ePrivacy Directive expressly refers to a subscriber or individual, meaning that not only subscribers but also third-parties concerned (for instance, those with whom subscribers communicated over the electronic communications network) as well as former users are to be notified in the event of a personal data breach.[155] Evidently, natural as well as legal persons could be subscribers or users for the above purposes.[156]

As far as the content of such notification is concerned, it "shall at least describe the nature of the personal data breach and the contact points where more information can be obtained, and shall recommend measures to mitigate the possible adverse effects of the personal data

152. They also constitute personal data, regardless whether dynamic or static; *see* 2009 Amending Directive, recital 52. The 2009 ePrivacy Directive, in the same Recital above, expressly points to the work done by the Article 29 Working Party; *see* Article 29 Data Protection Working Party, Opinion 2/2008 on the Review of the Directive 2002/58/EC on Privacy and Electronic Communications 4, 00989/08/EN, WP 150, May 15, 2008, *available* at, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2008/wp105_en.pdf (hereinafter "May 15, 2008 Opinion").

153. *See Second Opinion*, para. 31ff ("trigger for the notification" and the potential risks (over-notification) of making the system too sensitive).

154. 2009 Amending Directive, recital 61.

155. *See* May 15, 2008 Opinion; *Second Opinion*, para. 58.

156. 2009 Amending Directive. Legal persons, when using or subscribing to telecommunications networks, may be treated as individuals for the purposes of the ePrivacy Directive (see article 1.2), in strong antithesis with the Data Protection Directive, where data subjects may only be natural persons.

breach."[157] Additionally, it "should include information about measures taken by the provider to address the breach, as well as recommendations for the subscriber or individual concerned."[158] The notification should be transmitted "without undue delay," that is, as soon as the provider becomes aware that a breach occurred.[159] Given the urgent nature of such notification, the provider should use all and any means at its disposal to reach individuals, and not, for instance, rest upon a letter to all sent by post.

On the other hand, the national data protection authority (or any other competent authority in addition to that) ought always to be notified. No distinction or qualitative, quantitative, or alternative type of condition is introduced in this case. Once a data breach occurs, the electronic communications service provider should inform the state authorities as soon as it becomes aware of the breach. Evidently, the general provisions of national data protection acts continue to apply, and the data protection authority may impose fines or undertake other actions. According to provisions of the ePrivacy Directive, a timely and lawful notification by the provider does not prejudice the state authorities' further actions. In regards to its content, the notification to the competent national authorities should include all the aforementioned elements required for individuals as well as "describe the consequences of, and the measures proposed or taken by the provider to address, the personal data breach."[160]

Exemptions to the obligation to notify are introduced in the amended ePrivacy Directive, but only with regard to subscribers and users. These exemptions apply when the service provider has implemented appropriate technological protection measures. The "appropriateness" of these measures mostly consists in rendering the data unintelligible to any unauthorized person.[161] Evidently, these measures need to have been applied to the data compromised by the security breach. The decision regarding whether the above conditions concur is to be made by the data protection authority.

In view of the above, from a service provider perspective, the series of actions in the event of a personal data breach would be as follows: immediately when it becomes aware of the breach, the provider should

157. *Id.* at art. 2.

158. *Id.* at recital 61.

159. *See also* Barcelo & Traung, *supra* note 144, at 96.

160. 2009 Amending Directive, art. 2.

161. *Id.*; *see also* Article 29 Data Protection Working Party, Opinion 1/2009 on the Proposals Amending Directive 2002/58/EC on Privacy and Electronic Communications 6, 00350/09/EN, WP 159, Feb. 10, 2009, *available at* http://ec.europa.eu/justice/policies/privacy/dosc.wpdocs/2009/wp159_en.pdf (hereinafter "Feb. 10, 2009 Opinion") (for objections on the introduction of such exemptions).

notify the competent national authorities. If the provider is certain that individuals are affected, then it may proceed to notify them at the same time. If not, then it may defer by referring the matter to the national data protection authority. In cases where the provider has taken the precaution of encrypting its data, it may avoid notifying individuals. However, it ultimately rests with the data protection authority to decide where, irrespective of such data encryption, a notification indeed needs to take place.[162]

Providers may, therefore, find good reason in taking the precaution to encrypt their data, as it might save them from a costly and reputation-damaging public notification requirement. On the other hand, the amended ePrivacy Directive appears to be handing to service providers, perhaps unnecessarily,[163] valuable time to reflect. If a service provider has implemented some encryption system, it may declare it sufficient, avoid immediate notification, and wait for the national authority's instructions. In this case, service providers cannot be held liable for not timely notifying the individuals concerned.

In the meantime, the General Data Protection Regulation, in its first draft released by the Commission in early 2012, adopted the ePrivacy Directive's idea of using personal data breach notifications to warrant a more effective level of protection for individual data protection,[164] turning them into general personal data processing requirements. This development, if indeed the Regulation is ultimately adopted in its current wording, is expected to diminish the ePrivacy Directive's significance for the electronic communications sector, and thus create doubts as to the purposefulness of its continued existence altogether.

While releasing the amended ePrivacy Directive, the epicenter of disputes with regard to personal data breach notifications regarded the actual scope of this obligation. Data protection proponents, including the Parliament, the EDPS, and the Article 29 Working Party, persistently asked for this obligation to be extended to both electronic communications service providers and information society service providers.[165] Others (the Council and the Commission) insisted in burdening with this new obligation only the former.[166] In the end, the amended ePrivacy Directive made explicit reference only to electronic communications service

162. 2009 Amending Directive, art. 2.

163. *Second Opinion*, para. 50.

164. *See* ePrivacy Directive, arts. 4(9) & 31.

165. *See First Opinion*, para. 30; *Second Opinion*, para. 22; May 15, 2008 Opinion. The extension of the scope of the Directive to cover also information society services, normally addressed only to the telecommunications sector, was not considered a problem for its lawfulness, given that a number of its provisions are already extended in a similar way. *See, e.g.*, *First Opinion*, para. 33 and *Second Opinion*, para. 26.

166. *Second Opinion*, para. 13ff (highlighting the details for the different standpoints).

providers.[167] Therefore, only electronic service providers are bound by it.

However, this choice excludes significant information society players, namely the whole of the Internet. As noted by the EDPS, substantial personal data processing sectors (for instance, online banks, retailers, or health providers,[168] as well as social networks and search engines) are left out of these provisions, despite that, in the event of a personal data breach, individual data protection in their possession would be gravely infringed.[169] To this list should probably also be added, if at least the term "public communication networks" is narrowly interpreted, the various "apps" stores, yet another significant omission given the contemporary processing environment.

The only compromise granted to data protection proponents is included in the Recitals of the amended ePrivacy Directive, in the form of policy guidelines for the future.[170] There, it is noted that, although notification requirements are addressed only to electronic communications providers, such notifications reflect the general interest of individuals in order to better protect their rights.[171] All-encompassing mandatory notifications requirements should be introduced at Community level as a matter of priority, as such interest is clearly not limited to the electronic communications sector.[172] Once this extension of scope takes place, unless otherwise expressly provided, the aforementioned particulars of such a notification system shall apply to information society service providers as well. This case, however, constitutes further evidence that the ePrivacy Directive is by now struggling to get out of its suffocating boundaries with regard to the distinction between electronic communications service providers and information society service providers. This distinction is increasingly blurred in the contemporary processing environment.

The amended ePrivacy Directive explicitly describes the details for the setting up of a personal data breach notification system at Member State level. Specific actions are prescribed for both national data protection authorities and service providers.[173] As far as the former are concerned, they are encouraged to introduce guidelines and instructions

167. *See* ePrivacy Directive art. 4.

168. *See First Opinion*, para. 30ff; *Second Opinion*, para. 22.

169. *See also* Feb. 10, 2009 Opinion.

170. 2009 Amending Directive, recital 59.

171. *Id.*

172. *See id.*

173. *See* ePrivacy Directive, art. 4.4; *see also* Security Breach Notifications (PECR): Guidance for service providers, INFORMATION COMMISSIONER'S OFFICE (Mar. 28, 2012), http://www.ico.gov.uk/for_organisations/privacy_and_electronic_communications/security_breaches.aspx.

clarifying the notification particulars.[174] National data protection authorities are also authorized to audit the compliance of service providers as well as to impose sanctions in cases of default. For their part, service providers are instructed to establish an inventory detailing all circumstances and actions in response to personal data breaches.[175] Sector-specific guidelines and instructions (but not "technical implementing measures," as described below) issued by national authorities point to codes of practice and soft law schemes[176] aimed at creating consistency, while also protecting as much as possible individuals. The introduction of such instruments should not present difficulties, given that these provisions are aimed only at telecommunications providers and ISPs (and not to the chaotic Web 2.0 environment). The same guidelines and instructions could also include the appropriate forms for the providers' mandatory inventory of personal data breaches.[177]

In the same context, at the EU level the ePrivacy Directive introduces the notion of "technical implementing measures" to be adopted by the Communications Committee.[178] In effect, in order to ensure consistency among the different Member State approaches, the Commission may adopt technical implementing measures regulating the circumstances, format, and procedures applicable to the above personal data breach notification system.[179] These regulations shall be concluded in consultation with the European Network and Information Security Agency ("ENISA"), the Article 29 Working Party, and the EDPS, as well as relevant stakeholders, including the industry.

Without complicating this analysis by entering into the Comitology discussion,[180] it is enough here to note that these technical implementing measures in themselves are allowed to amend only non-essential elements of the ePrivacy Directive. When preparing them, due consideration should be given to the circumstances of the breach, any technical protection measures already in place, and to the concerns of law enforcement agencies so that early disclosure does not hamper the investigation of the circumstances of a breach.[181] Once formally adopted, these technical implementation measures are expected to create[182] an

174. *See* ePrivacy Directive, art. 4.4.

175. *See id.*

176. *See also* 2009 Amending Directive, recital 60 ("competent national authorities should monitor measures taken and disseminate best practices among providers of publicly available electronic communications services").

177. *See also* Feb. 10, 2009 Opinion.

178. *See* ePrivacy Directive, art. 4.5.

179. *See id.*; *see also* 2009 Amending Directive, recital 63.

180. *See First Opinion*, para. 35ff.

181. *See* 2009 Amending Directive, recital 64.

182. *See also First Opinion*, para. 38.

EU-wide common basis for the management of the notification process in the event of a personal data breach.

Altogether, however, it could be held that the data breach notifications system installed by the amended ePrivacy Directive is a complex system that may perhaps prove impractical when it comes to protecting individual data protection. The ePrivacy Directive goes into substantial depths while regulating, in detail, an otherwise straightforward obligation of service providers. Perhaps, being sector-specific legislation, it ultimately caters too much for its sector-specific needs and restraints. Given that a general data breach notification obligation for data controllers may find its way into the text of the amended Data Protection Directive,[183] perhaps the preferable way forward would be to abandon this highly technical and perhaps bureaucratic system in favor of simpler, direct notifications that will be required according to general, and not sector-specific, legislation by all and any data controllers who mishandle the personal data in their possession.

13. THE THREE STRIKES LAW DEBATE – THE INTERNET FREEDOM PROVISION

The so-called Three Strikes Law[184] debate is not directly connected to the ePrivacy Directive, as the actual provisions that were disputed are located in the Framework Directive of the Telecoms Reform Package. Nevertheless, despite the whereabouts of the relevant provisions, the debate was conducted almost entirely using data protection argumentation – yet another example where the existence of sector-specific legislation bound to a dynamic and ever-changing field does not ultimately assist data protection purposes. In view of the above, a brief note of the relevant background will be made here.

Three Strikes Laws describes the (European) Internet disconnection policies, whereby all ISPs are forced to install surveillance systems that track their client's online behavior (most likely by tracking their IP addresses).[185] Those that are found to be involved in unlawful exchanges of copyrighted or otherwise protected material are identified by the system and subsequently served a first written notice to abstain from any similar actions in the future. If the recipients of such notices do not comply, then they are warned one more time. If they continue to not comply, then

183. *See European Commission Communication.*

184. It seems, however, that the choice of name is rather unfortunate, because in the United States or Canada, where three strikes law have been enacted for years, they pertain to criminal justice laws. A more appropriate term would have probably been "graduated response" schemes.

185. *See 'Three-strikes' Law For Net Users*, BBC (Mar. 27, 2009), http://news.bbc.co.uk/2/hi/programmes/click_online/archive/7967689.stm.

their Internet access is automatically terminated or suspended.[186]

Three Strikes Laws were, at the time, suggested as a potential solution to the ever-increasing volume of unauthorized copyrighted file exchanges among users over the Internet (colloquially referred to as "Internet piracy"). These laws also, however, raise a series of data protection-related objections, in particular with regard to the proportionality or the purpose limitation principles.[187]

The original 2007 Commission proposal for the Telecoms Reform Package referred only indirectly to copyright protection in its Annex[188] without making any explicit reference to implementing three strikes law schemes. Nevertheless, the European Parliament, in its first reading in September 2008, expressly asked for an amendment that became known, per its numbering, as Amendment 138/46.[189] This Amendment specified that users are not to be denied Internet access by such automated means and make it impossible for Member States to enact similar laws at national level.

In early 2009, however, France decided to introduce into its national law relevant provisions.[190] As expected, it faced substantial objections while turning its Three Strikes initiative into national law.[191] It seems, therefore, that France placed considerable political pressure into turning the three strikes initiative into European law by means of incorporating it into the Directive (Telecoms Reform Package) that was already in the making. Such a tactic allowed France to avoid protests to its own national law.[192]

The intermediate period, until the Parliament's second reading, was highly political on this issue. National governments, Content Industry

186. *See also Opinion of the European Data Protection Supervisor on the Current Negotiations by the European Union of an Anti-Counterfeiting Trade Agreement (ACTA)*, par.15, 2010 O.J. (C 147) 1.

187. *See* Data Protection Directive, art. 6.

188. *See 2007 Proposal* ("In Point A.19 of the Annex: this allows NRAs to attach to general authorisations conditions concerning copyright and intellectual property rights.")

189. See, for instance, *Europeans Parliament Votes Against the 3 Strikes. Again*, EUROPEAN DIGITAL RIGHTS (May 2009), available at http://www.edri.org/edri-gram/number7.9/ep-plenary-votes-against-3-strikes.

190. These were referred to as "HADOPI" law. *See also* Alain Strowel, *The 'Graduated Response' in France: Is It the Good Reply to Online Copyright Infringements?, in* COPYRIGHT ENFORCEMENT AND THE INTERNET 147, 147-161 (Irini Stamatoudi ed. 2010); Valerie-Laure Benabou , *The Chase: The French Insight into the 'Three Strikes' System, in* COPYRIGHT ENFORCEMENT AND THE INTERNET 163, 163-179 (Irini Stamatoudi ed. 2010).

191. *See France's Three-Strikes Law for Internet Piracy Hasn't Brought Any Penalties*, N.Y. TIMES (July 18, 2010), http://www.nytimes.com/2010/07/19/technology/Internet/19iht-CACHE.html.

192. *See* Kevin J. O'Brien, *French Anti-Piracy Proposal Undermines E.U. Telecommunications Overhaul*, N.Y. TIMES (May 7, 2009), http://www.nytimes.com/2009/05/07/technology/07iht-telecoms.html.

lobbying, and NGOs, among others, were all actively involved into preserving or deleting Amendment 138/46.[193]

The European Parliament in its second reading, on May 5, 2009, upheld by vast majority (404 to 56) Amendment 138/46.[194] Given the Lisbon Treaty Environment, it enforced a compromise that would limit the implementation of Three Strikes Law schemes in the EU. This compromise was finally reached in the summer of 2009, after elections gave a new Parliament and a new Commission was formed.

The text of the Telecoms Reform Package now includes an "Internet Freedom Provision" in Article 1(3)a of the Framework Directive.[195] Access to the Internet for individuals in the EU thus appears safe from automated decision-making and related cut-offs. This provision, however, is the only protection for individuals that the Internet Freedom Provision firmly warrants: individuals will not be subjected to automated Internet disconnection decisions. The Provision does not prohibit per se the installation and use of surveillance systems by ISPs in order to combat Internet piracy.[196] The only thing it demands for such systems to operate lawfully, at least as far as it is concerned, is that any Internet

193. *Europeans Parliament Votes Against the 3 Strikes. Again*, EUROPEAN DIGITAL RIGHTS (May 2009), available at http://www.edri.org/edri-gram/number7.9/ep-plenary-votes-against-3-strikes.

194. *Id.*

195. Press Release, Agreement on EU Telecoms Reform Paves Way for Stronger Consumer Rights, an Open Internet, a Single European Telecoms Market and High-speed Internet Connections for all Citizens, MEMO/09/491 (Nov. 5, 2009, http://europa.eu/rapid/pressReleaseAction.do?reference=MEMO/09/491 (hereinafter "Nov. 5, 2009 Press Release").

> Measures taken by Member States regarding end-users' access to, or use of, services and applications through electronic communications networks shall respect the fundamental rights and freedoms of natural persons, as guaranteed by the European Convention for the Protection of Human Rights and Fundamental Freedoms and general principles of Community law". In addition, "Any of these measures regarding end-users' access to, or use of, services and applications through electronic communications networks liable to restrict those fundamental rights or freedoms may only be imposed if they are appropriate, proportionate and necessary within a democratic society, and their implementation shall be subject to adequate procedural safeguards in conformity with the European Convention for the Protection of Human Rights and Fundamental Freedoms and with general principles of Community law, including effective judicial protection and due process. Accordingly, these measures may only be taken with due respect for the principle of the presumption of innocence and the right to privacy. A prior, fair and impartial procedure shall be guaranteed, including the right to be heard of the person or persons concerned, subject to the need for appropriate conditions and procedural arrangements in duly substantiated cases of urgency in conformity with the European Convention for the Protection of Human Rights and Fundamental Freedoms. The right to effective and timely judicial review shall be guaranteed.

Id.

196. One should not forget that the Data Retention Directive makes use of similar systems for law enforcement purposes. *See* Section 6.

disconnection decision is made following a lawful procedure, including the right to be heard, and is subject to judicial review. Although it could be argued that these requirements make Three Strikes Laws slow, cumbersome, and ineffective when it comes to monitoring millions of copyright infringements on a daily basis, and thus in practice make their use impractical, the fact still remains that the Internet Freedom Provision in principle does not prohibit their use.[197]

Other shortcomings of the Internet Freedom Provision, when viewed from a data protection perspective, were duly identified, most notably its failure to regulate private parties as well and its vague reference to a "prior fair and impartial procedure."[198] These problems, however, could be solved either by making appropriate provision at national level or by providing judicial recourse to individuals.

In practice, the Telecoms Reform Package did not exclude Three Strikes legal schemes altogether in the EU, but, rather, set the minimum basis upon which they ought to operate. It attempted to provide a minimum level of protection for individuals while also striking a balance with lawful Content Industry requests. Member States are indeed allowed to carefully implement Three Strikes systems within their respective jurisdictions, if they so choose. Such systems, however, ought to observe the requirements of the (data protection) law.

Arguably, this was not a decision for the Telecoms Reform Package to make. The issue of the relationship between intellectual property law, as threatened in the contemporary Internet environment, and data protection law is a complex one that largely exceeds the electronic communications context.[199] The fact that the Telecoms Reform Package, while in

197. *See* Nov. 5, 2009 Press Release.

> According to the then competent Commissioner Reding, "the new Internet freedom provision represents a great victory for the rights and freedoms of European citizens. The debate between Parliament and Council has also clearly shown that we need find new, more modern and more effective ways in Europe to protect intellectual property and artistic creation. The promotion of legal offers, including across borders, should become a priority for policy-makers. 'Three-strikes-laws', which could cut off Internet access without a prior fair and impartial procedure or without effective and timely judicial review, will certainly not become part of European law.

Id.

198. *See Telecoms Package Amendment 138 compromise 20091105*, LA QUADRATURE DU NET WIKI, http://www.laquadrature.net/wiki/Telecoms_Package_Amendment138_compromise_20091105 (last modified Feb. 15, 2010, 2:42PM).

199. Case C-275/06, Productores de Musicia de Espana (Promusicae) v. Telefónica de Espana SAU, 2008 E.C.R. I-271, 2 C.M.L.R. 17 (2008); Kate Brimsted & Gavin 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,* 24 COMPUTER L. SECURITY & SECURITY REP. 275-279 (2008). The relationship in the EU between data protection and the numerous intellectual property protection initiatives undertaken either by the Content Industry or by national governments in order to combat Internet piracy is tense and largely

its lawmaking process, was forced to pick a side serves as yet another reminder that the annexing of sector-specific legislation to periodical electronic communications framework reviews does not ultimately assist the data protection purposes.

14. CONCLUSION

In 1997, the EU opted to amend its general data protection regime with a specific bill on electronic communications that was to be periodically amended. Indeed, the resulting ePrivacy Directive is currently in its third version, covering newly emerged issues of spyware, cookies, net neutrality, and even Internet piracy. However, since the release of its third version, in 2009, the EU data protection framework has entered a process of overall reform; this process is expected to be concluded by 2014. In parallel, the same is true with regard to the other basic data protection instrument in Europe, the Council Convention 108, that itself is undergoing an amendment process. Once concluded, these amendments are expected to gravely affect the provisions of the ePrivacy Directive.

Until such time, however, the current version of the ePrivacy Directive remains in effect – and still needs to be implemented at national level by several Member States. The 2009 amendment to the ePrivacy Directive via the Telecoms Reform Package ought to be assessed only after certain factors are duly considered. First, with regard to its *raison d'etre*, the amendment is the outcome of a periodical review process whose primary aim is to keep the main text of the Directive updated and relevant. In its current wording, the ePrivacy Directive is in its third version within some fifteen years since it was first released. The amendment under examination merely affected a few provisions in an already existing Directive. It neither replaced it altogether, as was the case between versions one and two, nor changed its numbering or name.

Second, as far as its subject-matter is concerned, the ePrivacy Directive's purpose is to make the broad principles of the Data Protection Directive concrete for the electronic communications sector. This creates both a limitation and an opportunity. The ePrivacy Directive can only apply, in a practical way, rules set elsewhere; it also needs to carefully follow the Data Protection Directive amendment process currently under way, in order to adopt its own provisions accordingly. On the other hand,

---

remains an unresolved issue. Understandably the Content Industry wishes to include ISPs in its efforts to protect its content from unlawful exchanges over the Internet, and would like to see them trace their clients' online behavior and act accordingly. Nevertheless, this does not sit well with European data protection law; unfortunately, the *Promusicae* case did not provide clear answers The issue is further complicated by the basic e-commerce principle in EU law on providers' liability; *see* E-Commerce Directive, arts. 13, 14, and 15.

the ePrivacy Directive addresses the needs of a sector at the forefront of international technical and financial developments. Although it cannot break new data protection grounds, it may resolve practical problems that affect the everyday lives of millions of people. At the same time, however, the ePrivacy Directive has to struggle not to appear prejudiced; that is, catering too much for the particular needs and restraints of the sector it regulates.

A third factor to take into consideration refers to the stakes at play. The ePrivacy Directive's provisions affect both millions of people and a number of the biggest companies in the world. A single change in the wording of even one of its minor provisions may cost billions of dollars and change well-established international business practices – not to mention the daily routine of all Internet users.

In view of the above, the amendment to the ePrivacy Directive through the Telecoms Reform Package, perhaps inevitably, constitutes a mid-term compromise between conflicting data protection and business interests. It should also be kept in mind that the potential release in the near future of a General Data Protection Regulation, if indeed in its current proposed wording, may turn several of the ePrivacy Directive's provisions obsolete, hence decidedly making a *lex specialis* for the electronic communications sector irrelevant.

Among the amendment's strengths, from a data protection point of view, is its brave establishment of a personal security breach notifications system, which is expected to assist individuals and state authorities when coping with an ever-increasing number of personal information leaks, as well as an attempt to remain technically relevant, through, for instance, explicit reference to RFID technology. The above, if seen from the industry perspective, mean substantial and costly additions to their business practices.

On the other hand, data protection objections mainly refer to the ePrivacy Directive's failure to adequately cover today's electronic communications' reality, i.e. the Internet. The convergence of all networks means in practice that the distinction between "electronic communications services" providers and "information society service" providers is by now obsolete.[200] Further complicating things for the ePrivacy Directive, these two terms seem to be mutually exclusive in the Telecoms Reform Package context.[201] The amendment itself does not make this distinc-

200. *See* May 15, 2008 Opinion.

201. *See* Framework Directive, art. 2(c) definitions:

> [E]lectronic communications service' means a service normally provided for remuneration which consists wholly or mainly in the conveyance of signals on electronic communications networks, including telecommunications services and transmission services in networks used for broadcasting, but exclude services providing, or exercising editorial control over, content transmitted using electronic communica-

tion, for instance, that "email service providers" are "electronic communications service providers" and not "information society service providers." Social networks sit awkwardly in this rigid scheme (despite the fact that electronic messages are exchanged between users of Facebook, LinkedIn, and similar applications). The same is true for apps. What is therefore desperately needed is a new Directive that accurately depicts this convergence and regulates the whole of the Internet space, as opposed to only parts of it.

Consistency is also damaged by the above, unjustified, distinction: the amended ePrivacy Directive's provisions on confidentiality of communications and spam expressly apply to everybody and not only to its regular entities – electronic communications service providers.[202] The Directive's data breach notification provisions apply to an extended circle of parties, equally exceeding its otherwise nominated recipients.[203] In addition, its provisions on cookies and spyware expressly apply to information society service providers as well.[204] Therefore, it would appear that the ePrivacy Directive is already desperately struggling to get out of its suffocating boundaries.

Other shortcomings from a data protection point of view refer to the regulation of private networks or the extent to which semi-public providers of electronic communication services are covered by the Directive's provisions.[205]

Data protection-related provisions are not necessarily located only in the ePrivacy Directive text. As already seen, the discussion on the Three Strikes regulatory implementations took place within the Framework Directive debate; equally, the Internet Freedom Provision is part of its text. Provisions on systems' integrity and security may be found in several locations in the Telecoms Reform Package. The ways that the Telecoms Reform Package affects individual data protection are numerous and well-exceed the limits of the ePrivacy Directive text.

This is probably the origin of data protection difficulties encountered in the amended ePrivacy Directive. It remains unproven whether the annexing of a data protection-specific Directive to a comprehensive, periodical "telecoms reform package" ultimately contributes to data protection purposes. The breadth of issues discussed and the stakes at play during

---

tions networks and services; it does not include information society services, as defined in Article 1 of Directive 98/34/EC, which do not consist wholly or mainly in the conveyance of signals on electronic communications networks.

Id.

202. *See* Directive on Privacy and Electronic Communications, arts. 5, 13, *as amended by* the 2009 Amending Directive.

203. *See id.*, art. 4, *as amended by* the 2009 Amending Directive.

204. *See id.*, art. 5.3, *as amended by* the 2009 Amending Directive.

205. *See First Opinion,* paras. 12 and 21.

the lawmaking process of such important legislation for contemporary societies at times move the focus away from individual data protection. Data protection thus becomes a negotiating tool in a struggle and balancing of powers not entirely related to it.

Even if seen from a confidentiality of communications point of view, notwithstanding the fact that this is rather a secondary aim of the ePrivacy Directive, a dedicated piece of legislation is perhaps an ineffective policy choice from a human rights perspective. Even if perceived as an end in itself, confidentiality of communications-relevant provisions will have to follow the general definitions and principles of the ePrivacy Directive. Consequently, all the aforementioned shortcomings with regard to the protection of the individual right to data protection equally apply regarding the protection of the individual right to confidentiality of communications. Because it is embedded in an otherwise data protection system within the ePrivacy Directive, the protection of the general right to confidentiality of communications can only lose if the system itself is fundamentally flawed.

Telecommunications may have been in line with the 1997 climate to introduce sector-specific data protection legislation. After some fifteen years have passed, however, it is the only sector to continue doing so. Other equally interesting data processing sectors, from a data protection point of view, such as banking or direct marketing, rely on the general provisions of the Data Protection Directive, complemented at national level by "soft" law. It appears, therefore, that the regulatory approach per se needs careful re-assessment. If the furthering of data protection is the primary concern behind the release of each new version of the ePrivacy Directive, perhaps this aim would be better served through a general reference to the Data Protection Directive broad principles, rather than risking, with the opening of each periodical amendment process, the introduction of privacy-intrusive schemes, such as Three Strikes Laws, in the text of an otherwise ePrivacy Directive.