# The CDSL Working Paper Series

WP1/2019

CYBER & DATA SECURITY LAB

# Big data analytics in electronic communications: A reality in need of granular regulation (even if this includes an interim period of no regulation at all)

*Vagelis Papakonstantinou & Paul de Hert*



This Working Paper to be published in the Computer Law and Security Review, 2020.

Reference to a CDSL WP should be made as follows: [Author(s)], [Title], CDSL Working Paper [number/year], available at https://cdsl.research.vub.be/en/publications

# Abstract

In this article, we provide an overview of the literature on chilling effects and corporate profiling, while also connecting the two topics. We start by explaining how profiling, in an increasingly data-rich environment, creates substantial power asymmetries between users and platforms (and corporations more broadly). Inferences and the increasingly automated nature of decision-making, both based on user data, are essential aspects of profiling. We then connect chilling effects theory and the relevant empirical findings to corporate profiling. In this article, we first stress the relationship and similarities between profiling and surveillance. Second, we describe chilling effects as a result of state and peer surveillance, specifically. We then show the interrelatedness of corporate and state profiling, and finally spotlight the customization of behaviour and behavioural manipulation as particularly significant issues in this discourse. This is complemented with an exploration of the legal foundations of profiling through an analysis of European and US data protection law. We find that while Europe has a clear regulatory framework in place for profiling, the US primarily relies on a patchwork of sector-specific or state laws. Further, there is an attempt to regulate differential impacts of profiling via anti-discrimination statutes, yet few policies focus on combating generalized harms of profiling, such as chilling effects. Finally, we devise four concise propositions to guide future research on the connection between corporate profiling and chilling effects.

# Table of Contents

## 1. Introduction

Big data analytics has been defined by the European Data Protection Supervisor, under a common denominator approach, as the practice of combining and analysing huge volumes of diversely sourced information ("big data") using sophisticated algorithms in order to inform decisions.11 Notwithstanding the discussion whether personal data constitute a new asset for companies,[2] the fact remains that organisations find new value through constant re-processing of personal data either already in their possession or coming from third parties.

Over the past few years big data analytics have forcefully entered the mainstream. Admittedly, modern life would be inconceivable without the services afforded by this type of processing in the field of electronic communications. Mobile phones, seamless access to the internet and optimised telecommunications services are in essence the basis upon which life as we know it today is built – something after all acknowledged also within EU's Digital Single Market strategy.[3] Nevertheless, none of the above would be possible without some type of big data analytics run in the background. In fact, continued and more intensive big data analytics is absolutely necessary in order to improve the already high standards of user experience each one of us is currently enjoying – and would presumably be quite reluctant to let go.

At the same time public administrations are increasingly discovering the benefits of big data analytics afforded to them by telecommunications operators: cities wish to know if their services are optimally used by their residents; or, if attendance justifies resources spent on an event; or, which streets are most frequented by drivers at which time of the day; or the geographical areas that hospitals, public parks or other facilities actually serve. The list is practically limitless, fed by an insatiable need by smart cities to know more of their citizens and optimise resources and services.

and optimise resources and services.

Despite public attention and high volumes of expert analyses on challenges to personal data protection by this type of data processing,[4] the majority of approaches remains theoretical. The actual operations indeed taking place within public or private organisations today remain largely unexplored. Perhaps this lack of information is to be expected given the fact that big data analytics is actually performed behind closed doors. Organisations are expectedly unwilling to disclose organizational details that constitute valuable business

1 European Data Protection Supervisor (EDPS), Meeting the challenges of Big Data – A call for transparency, user control, data protection by design and accountability, Opinion 7/2015, 19 November 2015, p.7.
2 For example, World Economic Forum, "Personal Data: The Emergence of a New Asset Class", 2011. This would however open up discussions on proprietary rights over personal data.
3 See the relevant European Commission site (and priority), at https://ec.europa.eu/commission/priorities/ digital-single-market_en. The GDPR and the ePrivacy legislation are both policies within EU's DSM strategy.

information. From their part, Data Protection Authorities ("DPAs") and legal scholars have to confine themselves to whatever information may be inferred from public announcements or, even, personal data breaches.[5] Tellingly, therefore, the EDPS speaks of the "black box" of big data analytics.[6] In the same context, both the Article 29 Working Party (by now, the European Data Protection Board - EDPB) and the EDPS have asked for an "innovative" mind-set from all parties concerned when applying data protection doctrine on big data analytics operations.[7]

A pragmatic analysis on big data analytics would have to be industry- specific. Although the computing theory behind it may be essentially the same, as far as data protection purposes are concerned the actual operational details matter. Sources of data, purposes of the processing, decision-making mechanisms or participating actors, including the recipients of the processing results, are all critical factors when it comes to the legal treatment of big data analytics operations. Because all of them differ substantially among industries any meaningful data protection analysis of these operations will have to take into account the particulars of a single industry each time.

Electronic communications actors ("*telecommunication network operators*" offering telephony and telephony-related services[8] and internet services providers that offer "*information society services*"[9]) are prime candidates, or even already prime users, of big data analytics. They sit on a wealth of subscriber information collected in their course of business. These data are, or can be, continuously re-examined in order to extract added value from them.

Processing of personal data in the electronic communications sector is regulated within the ePrivacy regulatory framework, under a *lex specialis/lex generalis* relationship with general data protection legislation, currently set by the General Data Protection Regulation ("GDPR").[10] At the time of drafting of this paper the regulatory process has admittedly not been in perfect synchronisation: while the GDPR has entered into effect since May 2018, the ePrivacy regulatory framework continues to be provided by the ePrivacy Directive.[11] A draft Regulation on Privacy and Electronic Communications,[12] that would among others harmonise the ePrivacy provisions with those of the GDPR, is yet to exit the law-making process. Even when this finally happens, an intermediate period until it enters into effect means that today's lack of harmonised provisions will continue for the foreseeable future.

The authors were able to open, and stare into, the "black box" of big data analytics in the electronic communications field in 2017 and 2018 in the context of GDPR compliance assessments. During this period, we were able to acquaint ourselves with actual practices, operations and objectives in the electronic

communications field, particularly as regards telecommunications operators.[13] Our knowledge and experience gained is incorporated into this paper and constitute the basis of our suggestions.

The first section in the analysis that follows will attempt to set the legal scene today, answering two crucial questions on scope and applicable law. The three subsequent sections will present a typology for a scalable and granular approach that we feel is necessary but nevertheless is absent from the text of the draft ePrivacy Regulation: this will be done first in terms of suggesting a classification for "electronic communication services" from an ePrivacy perspective (in Section 2), then in terms of the types of personal data that electronic communications actors process (in Section 3), and, finally, in terms of the big data analytics operations that they actually carry out (in Section 4). Subsequently, three challenges for the ePrivacy legal framework from a data protection point of view will presented in Sections 5–7, where the issues of consent, legitimate interest of the controller, data anonymisation, purpose limitation, as well as the processing of metadata are respectively elaborated.

On the basis of the above sections, we conclude that processing requirements and particularities, as evidenced under the big data analytics paradigm, make necessary a much more detailed approach than the one afforded by the draft ePrivacy Regulation today. While this may (or may not) be also true for its other sections, pertaining to confidentiality of communications, consumer rights or cookies,[142] we believe that the ePrivacy Regulation's data protection sections suffer from lack of specificity and detail. Until these needs are met, through the introduction of a new, fundamentally amended text, we suggest that the current regulatory

4 See, for example, Christopher Kuner, Fred H. Cate, Christopher Millard, Dan Jerker B. Svantesson, The challenge of 'big data' for data protection, International Data Privacy Law, Volume 2, Issue 2, May 2012, Pages 47–49, Omer Tene, Jules Polonetsky. Privacy in the Age of Big Data: A Time for Big Decisions, Stan. L. Rev. Online, 2011, Ira S. Rubinstein, Big Data: The End of Privacy or a New Beginning? International Data Privacy Law, Volume 3, Issue 2, May 2013, Pages 74–87, Alessandro Mantelero, AI and Big Data: A blueprint for a human rights, social and ethical impact assessment, Computer Law & Security Review, Volume 34, Issue 4.

5 See, for example, Fortune.com, The Latest Big Data Breach Should Make You Rethink How You Pay for Everything, 4 April 2019, Business Insider, The 21 scariest data breaches of 2018, 30 December 2018.

6 EDPS, Meeting the challenges of Big Data, ibid, p.10

7 Ibid, p.5.

8 The term is used here to denote providers, or operators, of "public telecommunications networks", in the meaning of, the old, Directive 97/66/EC – essentially, the fixed-line and mobile telecommunications network providers active in each EU Member State.

9 Providers offering Information Society Services as per the definition of Directive 2015/1535 (Article 1).

10 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1–88).

11 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ L 201, 31.7.2002, p.37), as amended and in effect today (henceforth, the "ePrivacy Directive").

12 European Commission, Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), COM (2017) 10 final, 10.01.2017 (henceforth, the "draft ePrivacy Regulation"

framework and the mechanisms afforded by it be extended for an interim period, so as to afford legislators with the necessary space and time to revise their work.

## 2. Setting the (legal) scene: two crucial questions on scope and applicable law

At the time of drafting this paper (early 2019), because of asynchronous law-making initiatives, two crucial questions may be raised within the EU ePrivacy legislation context: do internet services providers fall under EU ePrivacy law? And what is exactly EU ePrivacy law composed of today: the GDPR and/or the ePrivacy Directive?

As far as the first question is concerned, the ePrivacy Directive originally excluded internet services providers from its scope,[15] a policy option that attracted much criticism, particularly due to the fact that technological advances blurred the boundaries among internet market players.[16] At any event, the legal mechanism through which such exemption was carried out in its text was as follows: Article 3 of the ePrivacy Directive sets that "this Directive shall apply to the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks in the Community", whereby Article 2 leaves the task of defining what exactly such "electronic communications services" includes to other legal texts.[17] It was in these latter legal texts that the exemption of internet services providers was carried out.[18]

However, things changed in December 2018. In essence, the legal texts that Article 2 of the ePrivacy Directive pointed at were replaced by the EU Electronic Communications Code.[19] The EU Electronic Communications Code no longer excludes all internet services providers from its provisions. On the contrary, it has expanded the definition of "electronic communications services" to include also "interpersonal communications services".[20] In practice, as explained in its text, "electronic communications services such as voice telephony, messaging services and electronic mail services are covered by this Directive".[21]

Consequently, by virtue of the above dynamic mechanism it appears that the ePrivacy Directive now also applies over certain internet services providers, in particular those offering voice telephony, messaging services and e-mail services. Its Article 2 now pointing to the EU Electronic Communications Code, the latter's provisions apply also for all aims and purposes of the ePrivacy Directive.

The second crucial question, however, pertains to the ePrivacy Directive itself: after the GDPR came into effect in May 2018, and the draft ePrivacy Regulation still under law-making process, to what extent does it still provide substantive law in the EU ePrivacy field?

Back in 2009, when the last version of the ePrivacy Directive was released, the connection was clear: "The provisions of this Directive particularise and complement Directive 95/46/EC".[22] Now, however, that Directive 95/46 has been replaced by the GDPR, to what extent is "particularisation" still possible? Can a 2009 Directive "particularise and complement" a completely new and extremely detailed 2018 Regulation?

The GDPR makes forays into the ePrivacy field, for example when setting that location data are personal data;[23] It also asks that "once this Regulation is adopted, Directive 2002/58/EC should be reviewed in particular in order to ensure consistency with this Regulation",[24] indirectly thus acknowledging incompatibility. On the same topic, the GDPR sets that it "shall not impose additional obligations on natural or legal persons in relation to processing in connection with the provision of publicly available electronic communications services in public communication networks in the Union in relation to matters for which they are subject to specific obligations with the same objective set out in Directive 2002/58/EC".[25] On the other hand, legal certainty is warranted through its article 94, whereby any and all "references to the repealed Directive shall be construed as references to this Regulation". Where does this all leave us?

The European Data Protection Board has recently provided valuable guidance on this topic.[26] First and foremost for the purposes of this analysis, despite extensive material scope overlaps,[27] it acknowledges the possibility of co-existence of the two legal texts. In other words, the EDPB replied in the positive, whether the ePrivacy Directive may (still) "complement and particularise" the GDPR.[28] If one accepts that as sound legal theory premise, then a mechanism for co-existence between the two instruments need to be devised, as is indeed done by the EDPB in its Opinion.[29]

---

13 Processing operations and types of data described in this paper have been aggregated by the authors and are not actor specific. All classifications, categorisations and attributes of processing operations presented in this paper are the authors' alone, drawn to the best of their knowledge and ability. The authors assume all responsibility for technical or technological mistakes or misunderstandings found in this paper.

14 These sections are not covered in our paper.

15 With the exception of Articles 5(3) and 13 (a notable, if not unique case where a legal instrument on two particular provisions exceeds its otherwise general scope).

16 See V Papakonstantinou/P de Hert, 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 and Info. L. 29 (2011).

17 Directive 95/46/EC and Directive 2002/21/EC.

18 In article 2 of Directive 2002/21/EC.

19 That is incorporated into Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code, OJ L 321, 17.12.2018.

20 See its Article 2(4) (and (5), as regards the definition of "interpersonal communications services").

21 See its Recital 10.

22 Article 1.2 of the ePrivacy Directive. On the role of the ePrivacy legislation see also Poullet Y. (2010) About the E-Privacy Directive: Towards a Third Generation of Data Protection Legislation? In: Gutwirth S., Poullet Y., De Hert P. (eds) Data Protection in a Profiled World. Springer, Dordrecht

23 See its Article 4.1

24 Recital 173 of the GDPR.

25 Article 95.

The authors agree with the EDPB's approach, however, can only see it as a realistic solution for a short, interim period. The GDPR never anticipated long co-existence with the ePrivacy Directive, in fact it expressly asks for the exact contrary. Even if one chooses to disregard extensive material scope overlaps, the fact that the GDPR now sets what is acceptable or not in personal data processing cannot be overlooked; Substantive requirements in the text of the ePrivacy Directive ought not be taken for granted in the post-GDPR environment. Finally, as seen, the ePrivacy Directive was drafted ten years ago taking into account different recipients than the ones recently added to it by the EU Electronic Communications Code. Its provisions were drafted aiming at telecommunications operators whereas now a significant part of internet services providers has entered the picture. A complete overturn of both its legal framework of reference (the 95/46 Directive) and its recipients means that the ePrivacy Directive is by now hopelessly left behind. While an interim arrangement could be struck, the fact remains that a replacement is indeed needed; It therefore remains to be seen whether this role could indeed be undertaken by the current ePrivacy Regulation draft.

26 In its Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities, adopted on 12 March 2019.
27 See Chapter 3.3.
28 In paragraph 37.
29 See Chapter 4.4, particularly paragraph 45
30 In 1993, the EU and its Member States committed themselves to the liberalization of the European telecommunications services sector by January 1, 1998 (European Commission, Towards a New Framework for Electronic Communications Infrastructure and Associated Services, The 1999 Communications Review, COM (1999) 537 final (10 November 1999).
31 Other than the ePrivacy Directive this included most notably 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; 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; 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; 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; 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 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, OJ L 24, 30.1.1998, p. 1–8.
33 The ePrivacy Directive defines "value added services" as meaning "any service which requires the processing of traffic data or location data other than traffic data beyond what is necessary for the transmission of a communication or the billing thereof" (Art. 2(g)).
34 See also the examples of the ePrivacy Directive in Recital 18: Advice on least expensive tariff packages, route guidance, traffic information, weather forecasts and tourist information.
35 See its Article 4(1)(b), that expressly refers, in brackets, to the Code.
36 See Recital 18 of the draft ePrivacy Regulation (and also Recitals 213 and 237 of the European Electronic Communications Code (Directive 2018/1972, where this approach is further confirmed.
37 See Recital 18 of the draft ePrivacy Regulation.
38 See Article 2(g) of the ePrivacy
39 See G. Buttarelli, The urgent case for a new ePrivacy law, The EDPS Blog, 19 October 2018.

## 3. "Electronic communication services": a fresh look at a term in urgent need of classification

The ePrivacy regulatory framework dates since the 1990s when the EU telecommunications market was "liberalised"[30] through the first relevant legislative package,[31] part of which actually was the first ePrivacy Directive.[32] However back then the addressees of its provisions were explicitly referred to in its title and easy to distinguish: telecommunications operators. These included either the incumbent (the telecommunications state monopoly in each Member State) or these wishing to enter the same market as competitors. Each one of them essentially offered two types of services to its customers: voice communication and access to the internet, that was then still at its first infant steps.

Two developments, one technological and one business, took place during the last twenty years that blurred the above offering, opening up in the process the circle of actors concerned. From a technological point of view broadband internet connections made voice communication over the internet (IP telephony) possible. This development widened significantly the circle of organisations offering voice communication services to the public to include also non-traditional telecommunications operators (essentially, internet companies). On the other hand, the business development occurred within traditional telecommunications operators themselves: witnessing their market share drastically reduced by the above technological development, they enhanced their offering through value-added services[33] to their subscribers; these services were not shy of venturing well into internet companies' territory.[34]

This is more or less where the electronic communications market in the EU is found today: voice and internet access services are on offer by a multitude of players in the market. In fact, these services have become so commonplace that competition has driven prices as low as possible. More lucrative profit margins are to be found in value-added services, whereby consumers are prepared to pay a premium in return of, for example, geolocation services, video (television) services, handset-related services (upgrade/replacement), contract-related services (bundle sale, friends/family/company packages) or whatever new services new technologies and imaginative marketing departments may offer them from time to time.

This mix-up of actors and services, however, is the first market development that the ePrivacy regulatory framework fails to acknowledge. As explained above in Section 1, the definition of "electronic communication services" is left by the ePrivacy Directive to be performed in other legal texts: back in 2009 it was Directive 2002/21/EC that assumed this task, now it is the EU Electronic Communications Code. This is a law-making option maintained in the draft ePrivacy Regulation.[35] In other words, data protection-specific legislation allows third, unrelated legislative documents to define exactly who its addressees are.

While this law-making option may make sense in terms of remaining technologically updated (provided of course that the ePrivacy text keeps up with the other electronic communications legal texts, unlike what is happening today), it is not necessarily suitable also for the data protection field. If the aims of ePrivacy laws to "particularise" and "customise" general data protection provisions onto actual electronic communications circumstances are to be served, a far more detailed approach is needed in order to successfully regulate such complex cases as big data analytics. Such an approach is not necessarily found in third, unrelated legislative documents that, understandably, cater to different needs.

In particular, the draft ePrivacy Regulation seems to distinguish only between "essential" or "basic" electronic communication services: these are to include "basic broadband internet access and voice communications services".[36] The legislator's underlying thinking is that because these services are essential (i.e., everybody needs to have access to them) regulatory safeguards need to be higher to the benefit of individuals in fear of them not having a "genuine and free" choice and thus being "unable to refuse or withdraw consent without detriment".[37] However, in this way the draft ePrivacy Regulation effectively removed the "value-added services" that are found in the text of the ePrivacy Directive[38]– a policy choice that appears unjustified under current market conditions.

40 Acknowledging only "value-added services" as seen above.
41 A finding that could be useful as regards the "reasonable expectation of privacy" repeatedly assessed by the ECtHR (see, for example, the Copland v. the United Kingdom, and, more recently, Barbulescu v Romania cases).
42 Articles 6.3 and 9.1, respectively
43 In this context, the ePrivacy Directive asks for data anonymization in both traffic and location data processing, whenever possible (see its Articles 6 and 9, respectively).
44 Legal scholars have argued, as early as in 2010, that personal data anonymization is impossible anyway, see Paul Ohm, 'Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization', UCLA Law Review 57 (2010): 1701–59.
45 On the GDPR's pragmatic approach see Mike Hintze, 'Viewing the GDPR through a De-Identification Lens: A Tool for Compliance, Clarification, and Consistency', International Data Privacy Law 8, no. 1 (1 February 2018): 86–101.
46 On the issue of data anonymization see also Sophie Stalla Bourdillon and Alison Knight, 'Anonymous Data v. Personal Data – False Debate: an EU Perspective on Anonymization, Pseudonymization and Personal Data', Wisconsin International Law Journal 34 (2017 2016): 284.
47 Recital 26. See also Article 11. On the issue of data anonym see, among others, S Stalla-Bourdillon/A Knight, Anonymous Data v. Personal Data — A False Debate: An EU Perspective on Anonymization, Pseudonymization and Personal Data, Wisconsin International Law Journal, 2017, P Ohm, Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization, UCLA Law Review, Vol. 57, 2010;
48 CJEU, Patrick Breyer v Bundesrepublik Deutschland, C-582/14, 19 October 2016.
49 Ibid, par. 49.
50 Ibid, par. 46.
51 As the only humanly possible way for two legal persons to interact
52 See its Article 6.4.
53 G. Buttarrelli, ibid.
54 As per its definitional approach, electronic communications data overall are to be comprised by electronic communications content and electronic communications metadata (see its Article 4).
55 Preamble, 2.
56 G Buttarrelli, ibid

While distinguishing "basic" electronic communication services may have been a valid (and worthy) approach in the 1990s, when voice and internet access services were provided by only a handful of (telecommunications) providers in each Member State, this no longer is the case. Today, internet access and voice communication are on offer by a multitude of providers (see, for example, Wi-Fi networks or internet telephony respectively), most of which not in the form of traditional telecommunications companies.

The ePrivacy regulator's viewpoint needs therefore to be updated: if technological developments have long now enabled multiple providers to offer voice services and internet connectivity to the public, then these two are simply no longer "basic" or "essential" services in need of regulatory protection. Instead, there is an abundance of offers and options. In other words, providers of these services, because they openly compete in the market, do not need to be given regulatory instructions, how to organise their business models, on top of already very competitive market constraints. In even more practical terms, if an organisation decides to combine consent to process data with free access to the internet the legislator has no reason to intervene (detrimental withdrawal of consent) because the individual concerned can simply move to a different provider if it does not wish to take this offer.

The ePrivacy regulator therefore needs a better classification among electronic communication services, that essentially takes little account of actors but focuses on the services on offer instead, perhaps as follows:

| **Service**<br>(To be expressly included and regulated in ePrivacy legislation) | **Attributes**<br>(Regulation to take place under the following understanding) |
|---|---|
| **Basic/essential services** | Voice and internet access, on offer by a multitude of providers (including SMEs) and through a multitude of technological solutions |
| **Necessary services** | A series of services (for example, security, fraud detection, signal improvement, customer care, technical support) that are related and necessary for the provision of the basic services |
| **Value-added services** | Any and all services not falling under the above two categories |

An explicit distinction among services, as above, has the advantage of enabling a layered regulatory approach: while basic services could be essentially left open to market competition (the tying up of individuals feared by the legislator long now being irrelevant), some types of value-added services could indeed be more strictly regulated. Classification brings flexibility, which is a much-needed trait in a piece of legislation that aims at regulating such a vast and dynamic field. However, this is a task to be carried out under the ePrivacy legal

framework, that can no longer depend on the definitions found in other legal acts to do it: the level of specificity needed for data protection purposes cannot (and should not) be met in general electronic communications EU laws.

## 4. What types of personal data do electronic communications actors process?

The second failure of the ePrivacy regulatory model to keep up with business developments refers to personal data classification and processing circumstances. On the one hand, telecommunications operators, in spite of the grave changes in market conditions, have more or less kept their basic business model intact: customers are invited to enter long-term contracts for the provision of voice and/or internet access and/or addedvalue services. On the other hand, internet service providers, being newcomers in the field, have applied a forceful new "free" business model, whereby their basic services are provided for free in exchange of increased processing of personal data.

The categories of personal data processed under the ePrivacy regulatory framework are therefore as follows:

| **Categories of personal data** | **Attributes** |
|---|---|
| Subscriber data | Personal information requested from and provided by subscribers during the application and execution of a new contract. |
| Metadata | Use of services data, potentially including any or all the following categories:<br>- Numbers dialled.<br>- Internet sites visited, URL-related data.<br>- Location data / data related to the connection point of the terminal equipment.<br>- Use of services data.<br>- TV channels viewed.<br>- Date, time, duration of the communication(s).<br>- Type of the communication(s) (voice or data). |
| Content of communications | Voice call content, SMS text, voice mail message, email content. |

Understanding the above categories of personal data is important while delineating the processing of telecommunications operators against that of internet service providers. Although, as seen, by now they both fall under the ePrivacy framework, their personal data processing differs substantially. In practice:

| **Categories of personal data** | **Telecommunications operators** | **Internet services providers** |
|---|---|---|
| Subscriber data | Detailed (in order to enter formal contracts for the provision of telecommunications services). | Limited (most of the time only name and email address). |
| Metadata | Vary considerably, on a case per case basis, for example:<br>Telecommunications operators have detailed data on number dialled/date/time/duration of a voice call.<br>Internet service providers have better geolocation data, because they use GPS instead of cell tower triangulation. | |
| Content | In principle not processed (unless required by law) | In principle processed (e.g., in free email services) |

In essence, the quality of the processing differs because of the different business models underlying it. Telecommunications operators are paid a fixed amount in long-term contracts based on service usage, while internet service providers often offer their services for free in, implied, return of increased personal data processing to be used in advertising. So, while for the former intensive personal data processing is a by-function (quality of the voice or bandwidth being far more important so as to keep their customers) for the latter maximisation of the personal data processing is crucial (in order to offer a competitive advantage to their customers who are advertisers, not individuals).

This is a basic, fundamental distinction, also acknowledged by the EDPS, who notes that "traditional electronic communications services – fixed line and mobile telecommunications providers – have long been subject to clear limitations […] Companies within the category of information society services have been able to grow rapidly thanks to loopholes in our current legal environment".[39] While this distinction in no way justifies more relaxed data protection obligations upon telecommunications operators, it does support the need for increased specificity in the ePrivacy regulatory framework that goes much beyond the level achieved today in the draft ePrivacy Regulation. Unless its text is amended to meet this need for an updated, particularised approach it will not offer any added-value in the electronic communications field.

## 5. What types of big data analytics operations are run by electronic communications actors?

Big data analytics operations run by electronic communications actors today could be categorised as follows:

| **Personal data processing operations** | **Attributes** |
|---|---|
| Billing and customer support | Processing of personal data when entering a contract with a new client (natural person); Data provided directly from them. Processing may include correlation of data with other sources of information, for example against bad debtor databases.<br>Data are used in the normal flow of contract execution (e.g. complaints or questions by clients, payment notifications, roaming processing when travelling abroad).<br>Billing-related processing is frequently mandated by other fields of law (tax law, consumer law etc.). |
| Internal marketing processing | Processing performed for marketing purposes. It includes, for example, the processing underlying offers on contract renewals, upselling (e.g. offer for a new contract based on actual use of the service, premium contracts/users) and cross-selling (e.g. "family-and-friends" packages, other relevant offerings by the same provider).<br>Not ongoing but triggered at contract renewal anniversaries.<br>Sometimes this type of processing is based on legal obligations by other fields of law (e.g. telecommunications law on tariff simulators). |
| Customer-insight models | Processing aimed at providing electronic communications actors with better knowledge on use of their services by their customers. They address management questions such as "*why clients call our customer service the most*" or "*what are the top reasons clients are leaving us*".<br>Fraud-detection or bad device detection processing falls under this category.<br>Run on an ongoing basis, depending on the questions asked.<br>They may include participation (and thus raise awareness) of clients (for example, through online questionnaires or phone surveys) but they may also be run silently on the background based on personal data that providers are already in possession of. |

| | |
|---|---|
| Processing for third parties | As a source of income<br><br>Used by internet service providers as an integral part of their business model; Never (or marginally) used by telecommunications operators.<br><br>Level of income depends on processing results, therefore there is clear motivation for increased levels of personal data processing. |
| | For other purposes<br><br>This is a relatively new type of processing that does not form any substantial part of business models for electronic communications actors but however can yield important social, financial and research findings. While processing is performed on actual data of individuals, usually the third parties that mandated the processing only access aggregated, anonymised information. Examples would refer to smart city applications, whereby questions such as "*how many visitors attended an event*" or "*recurring visitors to a festival*" or "*visitors from abroad to a local event*" or "*number of drivers using a specific road*" or "*residents' engagement with a public policy*" or "*optimal ways of citizens' engagement*" may be answered. |

All the above operations could conceivably qualify as "big data analytics" operations under the definition set in the introduction of this paper (combination and analysis of huge volumes of diversely sourced information to inform decisions). Electronic communications actors, particularly telecommunications operators and big internet services providers, may count millions of customers. These customers use their services intensively, multiple times per day, creating thus huge volumes of data in the process. Any adequate provision of the above services would have to combine competently large volumes of diversely sourced data if it was ever to achieve its purposes.

If placed next to the services and personal data taxonomy discussed above the following table could be drafted:

| **Big data analytics operation** | **Personal data used** | **Type of service** |
|---|---|---|
| Billing and customer support | Subscriber personal data<br>Metadata | Basic/essential service |
| Internal marketing | Subscriber personal data<br>Metadata | Basic/essential service<br>OR<br>Necessary service |

| | | |
|---|---|---|
| Customer-insight | Subscriber personal data<br>Metadata | Necessary service<br>OR<br>Value-added service |
| Processing for third parties | Subscriber personal data<br>Metadata | Value-added service |

The above table illustrates both the problems the ePrivacy legislator is faced with and the shortcomings of the current ePrivacy Regulation draft. In essence, metadata are used in all types of big data processing above, so there is a clear need to further distinguish among them. In essence, we need to walk along and further the ePrivacy Directive's path towards specificity[40] and not abandon it altogether.

A specific and detailed ePrivacy framework, having distinguished among metadata, would also offer valuable guidance as to services' categorisation. The industry's views as to which of its services, and thus processing operations, are today necessary and which are value-added may differ substantially to public perception. Plainly put, the industry may consider that customer insight is a necessary service in order for it to survive the market, whereas individuals, even among its own customers, may disagree. This is where the ePrivacy legislator ought to step in, in order to provide concrete and specific instructions on how best to deal with them from a data protection perspective.

The same would be the case, after all, in the event of a "spill-over" effect. Big data analytics processing may potentially be used in order to make correlations by reusable data. For example, processing carried out in the context of a basic service (billing) could be used in a customer-insight model (value-added service). Or customer support processing by one actor could be used as a marketing tool by another, to whom data have been transmitted. While the authors' predisposition would be that in the event of spill-over effect the stricter rules apply, particularly as regards actors' liability, here too specificity and granularity would allow the ePrivacy legislator to intervene, allowing or prohibiting or introducing specific safeguards for specific types of big data analytics processing.

The overarching principle here is specificity and granularity. We believe that the ePrivacy legislator needs to go deeper into actual processing circumstances in the electronic communications field. Of course, we do not believe that the ePrivacy Regulation should be turned into a technical document. A certain level of abstraction is necessary in order for the new ePrivacy law (or any law for that matter) to operate in practice. However, we believe that by looking more closely into types of data and categories of processing the ePrivacy legislator may achieve specificity without sacrificing generality. The frequent reviews of the ePrivacy regulatory texts, observed almost without failure until today, warrant that any choice the legislator makes today will be followed up and updated in the future.

Two further points merit special mention here. The first pertains to public expectations. If the authors are to be considered an indicative sample, it could be claimed that only some of the above personal data processing operations are perceivable, or even imaginable, by individuals.[41] This mostly refers to the first two categories (billing, customer service and simple marketing), whereby a reasonable level of customer knowledge and awareness is to be expected. However, this is most likely not the case with the last two categories of processing (customer-insights and third parties' processing), whereby customer knowledge and awareness ought not be taken for granted – as, after all, indicated by the increased journalistic interest such processing attracts from time to time.

The second point refers to the grave differences in the above personal data processing operations caused by the fundamentally different business models applied by electronic communications actors. In essence, telecommunications operators are far less likely to transfer their customers' personal data to third parties than internet service providers. This is on account of their business model and culture: Because they are long-established enterprises of large volume (some of them having been the only operator in a country for decades) they rarely feel the need to share their data or ask for data from third parties. On the other hand, internet service providers, not benefiting from fixed revenue through long-term contracts, are obliged to share the personal data of their customers with third parties – actually, their true and only paying clients, advertisement companies.

## 6. First challenge to the future ePrivacy regulation: the pursuit for big data analytics lawfulness – the cases of consent, legitimate interest of the controller, and data anonymisation

Even if specificity was indeed achieved in an ePrivacy regulatory text, perhaps along the lines described above, the ePrivacy legislator would still have to face a series of regulatory difficulties. In other words, the tasks of an ePrivacy regulatory text do not stop at competently classifying types of personal data and processing operations or distinguishing among its addressees: even if success was met on this front, a number of important issues would still have to be dealt with in order to efficiently address big data analytics circumstances.

A first and foremost challenge refers to lawfulness of the (big data analytics) processing. Any personal data processing under EU data protection law has to be based on a lawful basis. These are outlined in Article 6 of the GDPR: consent, performance of a contract, legal obligation of the controller, vital interests of the data subject, public interest, and legitimate interest of the controller. Unless one of them applies, under its own

terms and conditions, the processing will not be lawful. Admittedly, the ePrivacy Directive limits the lawful grounds for the processing of traffic and location data (the former, for marketing or provision of value-added services) to data subjects' consent only.[42] This policy option is preserved mostly intact in the Commission's draft ePrivacy Regulation, despite protests by the industry.

Big data analytics operations run in the electronic communications field are in need of a legal basis so as for them to lawfully take place. An obvious way out would be to have providers ask for their subscribers' or users' consent to participate in such processing. This is however the least practical solution. Individuals customarily neglect to respond to any requests for consent. This can be for a variety of reasons (implied refusal being of course a prominent one among them) however the fact remains that any such operation would yield very limited results. On the other hand, any attempt by providers to tie this consent with a financial offer or even threat of termination of contract could be interpreted as against Article 8 of the GDPR.

In view of the very limited practicability of consent electronic communications actors could make use of other legal bases for carrying out their big data analytics operations. The legitimate interest of the controller could perhaps serve them to this end. Notwithstanding whether this lawful ground finally makes it into the ePrivacy Regulation's text, and in spite of the ePrivacy Directive today not allowing it, here it should be noted that, even if that were the case, it should be used with caution: careful balancing needs to be made between the right to data protection and the need indeed of a provider to run a particular data analytics operation. This need may be evident for some but most likely not for all of the types of big data analytics operations run today. In addition, use of this legal basis involves a disproportionate risk for providers because they cannot be certain whether they are lawful or not unless a DPA, or a court, judges upon a concrete case – at which time, however the risk of already run operations will be huge.

However, the risk of already run operations will be huge. In lack of suitable legal basis electronic communications actors would obviously have to abandon the idea of conducting big data analytics operations altogether. In spite of the absurdity of this proposition, that creates as much a problem for the industry and for data protection itself, a solution could perhaps be to anonymise the data: Because the GDPR applies only to personal data tied to an identified or identifiable individual, anonymous data lie outside its scope.[43]

Nevertheless, anonymisation is not a viable option either, because anonymised personal data lose their value to such extent as to render big data analytics findings irrelevant. Out of the four categories listed above at most one could be based on anonymised data: billing and customer support and internal marketing operations are simply inconceivable without being able to process actual personal data. The same is the case most of the times with regard to customer insight models, that indeed need to refer to actual, identifiable individuals,

unless of course bulk questions such as handset compatibility or bad device detection are concerned. Only while processing for third parties could electronic communications actors anonymise their data, particularly given the fact that third parties are only provided with aggregated results; even in this case, however, it is doubtful whether at any moment of the processing (re-)identification of individuals would not be possible.

It is exactly this last difficulty that ultimately makes anonymisation a non-viable solution for big data analytics run in the electronic communications field. It refers to the inherent difficulty, if not impossibility, to anonymise personal data.[44] This is the result not so much of the GDPR's wording,[45] as to the restrictive interpretation adopted by the Article 29 Working Party (by now, the EDPB) on this matter – as in the meantime vindicated also by CJEU case law.[46]

The GDPR excludes anonymous information from its scope and introduces a proportionality criterion thereof, "on reasonably likely to be used means to identify a natural person".[47] Such "reasonableness" appears to allow for the necessary flexibility for controllers to apply measures in order to somehow achieve data anonymisation. Nevertheless, the Article 29 Working Party had raised the bar considerably with regard to anonymous data: "Anonymisation of data cannot be achieved by just stripping a dataset of some directly identifying attributes. The bigger and the more comprehensive a collection of data becomes, the more possibilities exist to identify the individuals whom the data relates to, especially when data is retained for longer periods of time and/or shared". The notion of "linkability" is used by it in this regard: "[consent would still be required] if the data are simply hashed, aggregated on an event level or otherwise pseudonymized, but there remains a possibility to single out users, or linkability of individual events in the aggregated data to the original data, also if future collection of traffic or location data creates linkability to events in the aggregated data set".

This restrictive interpretation has been confirmed by the CJEU: In Breyer[48] the Court ruled that "where [the latter] has the legal means which enable it to identify the data subject" then this is a case of an "identifiable" data subject and therefore EU data protection law applies.[49] Accordingly, such "legal means" exist whenever "identification of the data subject [is not] prohibited by law or [is made] practically impossible on account of the fact that it requires a disproportionate effort in terms of time, cost and manpower".[50] Consequently, given that an appropriate legal basis (law or contract) shall at all times exist[516] and because big data strives to

57 See its Article 9, "special categories of data".
58 After all, it could be argued that of similar or even higher importance than metadata are grocery stores' shopping lists based on loyalty cards, public libraries' book lending lists, etc.
59 See its Articles 6 and 9, respectively.
60 In its article 4.2(c)
61 On 7 December 2017 and 26 September 2018.
62 On 22 February 2018.
63 Vagelis Papakonstantinou/Paul de Hert, Big data analytics by telecommunications operators and the draft ePrivacy Regulation, Brussels Privacy Hub Working Paper N.13, September 2018 (available at https://brusselsprivacyhub.eu/publications/wp413.html).

minimize exactly such "disproportionate effort", identifiability ought to be considered a given at all times. Therefore, data anonymization is effectively never possible.

Although this interpretational eradication of any possibility for data anonymization could be considered contra legem, because the GDPR expressly allows for it,the fact remains that electronic communications actors cannot reasonably expect to use it in order to warrant lawfulness to their big data analytics operations under any circumstances whatsoever.

This would therefore be another topic ripe for the ePrivacy legislator's intervention. While there is no added value in repeating what is already in effect under the GDPR, as is the case with the current draft ePrivacy Regulation, an ePrivacy law could add scalability and granularity to this general and broad approach. For example, it could apply a principle whereby personal data remain anonymous as long as there is no indication that linkability becomes a risk. This would be a much more nuanced and compatible to market (if not reality) approach: if all data are at all times somehow "identifiable" to an individual then perhaps we need to go beyond that and examine the cases when this does not create a data protection problem. EPrivacy addressees would then be invited to apply the relevant measures in their practices.

The above are not meant to imply in any manner that electronic communications actors should be allowed to disregard the data protection safeguards altogether. Perhaps a practical and scalable approach would make most sense in this regard: New contracts and renewals could be accompanied by detailed and informed consent of users or subscribers at least for the type of data analytics operations that providers already know they are conducting. Whenever (and if) the legal basis of legitimate interest is to be used other data protection rights could be strengthened, such as the right to information through public media campaigns on the type of processing to be carried out or other means of informing the public. And, if anonymisation of the data can indeed take place without reducing the validity of findings for any given data analytics operation then it should indeed be applied; In addition, security and encryption measures could enhance compliance. We believe that any combination of the above measures, on an ad hoc basis, would achieve the right balance between protection of the individual right to data protection and taking advantage of the merits of big data analytics in full.

64 The EDPS, The urgent case for a new ePrivacy law, ibid

## 7. Second challenge to the future ePrivacy regulation: the principle of purpose limitation and big data analytics

The basic data protection principle of purpose limitation creates an inherent problem as regards the lawfulness of big data analytics. Article 4 of the GDPR requires that "*personal data be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes"*. However, as per their definition these operations typically combine and analyse "*huge volumes of diversely sourced information";* If personal data are "*diversely sourced"* then it is very likely that they were collected for different purposes than to participate in a big data analytics operation.

Some flexibility is provided in the GDPR by reference to the notion of "*further processing*".[52] Processing for a purpose other than that for which the personal data have been collected is permitted, even without data subjects' consent, when the new purpose is compatible with the initial. In order to verify whether this is the case either any link to the original purposes or the context and relationship between data subjects and the controller need to be assessed.

The Article 29 Working Party recommended that compatibility should be assessed in the light of the context in which the data were collected, of reasonable expectations of the data subjects, of the nature of the personal data in question, of the impact of further processing, and of safeguards to protect the data subject.

As regards big data analytics in the electronic communications field, it appears that the ePrivacy Directive allowing the marketing and value-added processing of location and traffic data only upon individuals' consent considers such processing incompatible to *"further processing*" as analysed above. The Commission's draft for an ePrivacy Regulation through copying of its approach apparently follows in its path. The EDPS has also issued an opinion critical of permitting *"further processing of metadata for compatible purposes*", because "metadata could be used for any purpose that is judged by the service provider to meet the 'compatibility' clause. In effect this could devalue the limited safeguards of the GDPR".[53]

On the other hand, a reading of the GDPR's provisions could support that several (but not all) of the processing operations listed above under 2 would indeed qualify under its "*further processing*" criteria. It is therefore difficult to explain to the electronic communications industry why its processing should have double standards if compared to, for example, the financial or the health industry.

We believe that here, again, granularity and scalability are of central importance. Big data analytics operations, particularly those pertaining to customer insight or catering to third parties requests may address entirely different questions each time and it is simply not reasonable to expect either before-hand knowledge

by those running them or, once a business decision is made to run such an operation, ad hoc consent to be provided by the millions of subscribers whose personal data are directly or indirectly affected. A possible way out of this impasse would be for detailed guidance to be provided to electronic communications actors: Having placed under broader categories their processing needs, the legislator could allow some operations under a *"further processing*" criterion, place higher compliance standards on others, and ask for explicit consent for those types of processing causing the highest risks for individuals. Such a level of specificity and granularity would be a task of an ePrivacy law – which unfortunately the current draft ePrivacy Regulation fails to meet.

## 8. Third challenge to the future ePrivacy regulation: the processing of metadata in need of a broader mandate

Metadata refers broadly to data ancillary to the main service provided each time by electronic communications services providers. The fact that they are ancillary does not mean that they are unimportant. In fact, their collection and processing is a necessary part for the provision of the service under consideration. However, the content of communications being by now constitutionally protected as a basic human right, attention unavoidably was turned to all peripheral information that can be, and is, collected and processed in a meaningful manner.

Electronic communications actors collect and process the types of metadata listed above (indicatively, location and traffic data, use of services, URL-related data etc.). The list may be dynamic, with new fields potentially added to it at the release of new technologies and/or services, but not so much: in fact, if we were to distinguish between the "basic" services of voice and internet access then the metadata list is quite fixed and will most likely continue to be so in the foreseeable future. The same being necessarily applicable also for the "necessary services" connected to the provision of "basic" services, it is value-added services, as per the distinction above, that are most likely to bring changes to the list.

Metadata are, undoubtedly, personal data under the GDPR definition, because they pertain to an identified or identifiable individual. They therefore fall squarely under data protection law. In addition, being particular to electronic communications, they are found at the epicentre of the ePrivacy regulatory framework's scope. Indeed, both the ePrivacy Directive (as regards location and traffic data) and the draft Regulation released by the Commission expressly aim to regulate metadata, the latter in fact making them a basic component of its structure.[54]

Having established that metadata are personal data, the next question is whether they are in any way exceptional. In other words, whether their particular characteristics makes it necessary for special provisions to apply to them, different than the general provisions on personal data processing introduced by the GDPR.

The Commission seems to believe so. In its draft ePrivacy Regulation it states that "*similarly [to the content(!) of electronic communications], metadata derived from electronic communications may also reveal very sensitive and personal information. These metadata include the numbers called, the websites visited, geographical location, the time, date and duration when an individual made a call etc., allowing precise conclusions to be drawn regarding the private lives of the persons involved in the electronic communication, such as their social relationships, their habits and activities of everyday life, their interests, tastes etc.".*[55] Accordingly, the Commission goes on to place special requirements for their lawful processing, essentially based on necessity for the provision of the services or subscribers' consent. Admittedly, the Commission here follows the ePrivacy Directive's approach on this matter, therefore its position should not be considered inconsistent.

The EDPS largely agrees with the Commission's approach: "*Location data reveals every movement, shows where we live, work and shop, which bars and restaurants we attend, which political events we attend, which medical services we need. Such metadata on when, how often and with whom we exchange messages and calls reveals our entire social position: who are good friends, how close are we with our family members, how much time we spend at work or with private contacts". Accordingly, he names metadata individuals' "most private information*".[56]

A formalistic reply to the Commission's or the EDPS' approach would be that it is contra legem: the GDPR recognizes only two types of data and the list of "sensitive data" is fixed,[57] a *lex specialis* cannot circumvent a *lex generalis*, and it would be anyway unwise to tamper with this list because no one can tell who might attempt to tamper with it next once the way to do it is shown.[58] Notwithstanding this, perhaps legalistic, reply, the fact remains that the processing of metadata poses an increased level of risk for individuals – and risk is indeed an assessable quality under the GDPR.

The lawfulness (or unlawfulness) of the approach aside, the Commission's approach on the processing of metadata also fails to acknowledge technical, and technological, specificity. Not all metadata are the same. For example, location data could reveal religion if an individual is spotted entering a church, however the technology used by telecommunications operators only provides a several hundred meters approximation of location – therefore, the church could well be the pub or the stadium close to it. GPS data used by internet services operators are far more exact in this regard. Also, not all metadata potentially reveal sensitive data.

For example, use of the services data (numbers dialled and duration of a call) cannot easily be used to this end (unless one is willing to profile an individual, if for example systematic calls are placed to a church, which is however also an ad infinitum loop). On the other hand, URLs can be far more revealing on an individual. Finally, some technologies, for example Wi-Fi networks, by design collect data of all passers-by and not only consenting customers.

Instead of acknowledging specificity, both the ePrivacy Directive and the draft Regulation have adopted a blanket approach with regard to metadata. The Directive merely distinguished between *"traffic*" and "l*ocation*" data.[59] The draft ePrivacy Regulation, rather than furthering and detailing this approach, abolished it altogether instead, aggregating any and all metadata under its *"electronic communications metadata*" definition,[60] awarding them the same treatment in bulk.

Nevertheless, here again granularity and specificity is critical. Not all metadata are the same: location data are more riskprone than duration of calls data. Not all technologies are the same: telecommunications operators use a technology that gives far less accurate results (to the point of irrelevance as far as location is concerned) than internet service providers. Finally, not all data analytics operations are the same: certain metadata processing is needed for provision of basic or necessary services described above. None of the above are acknowledged or taken into account in the draft ePrivacy Regulation text. However, specificity of regulation is its only reason for existence. If it fails to acknowledge actual processing specificities, equating telecommunications operators with internet service providers, or if it is left behind in basic technical specifications then there is simply no reason in persisting on keeping it – at least in its currently suggested wording.

## 9. Conclusion: our modest proposal for a new, specific and hopefully more effective data protection provisions in the ePrivacy regulation

While assessing GDPR compliance back in 2017, using also the draft ePrivacy Regulation text released at that time, the authors were faced with a simple, yet difficult to reply, question: are big data analytics operations in the electronic communications field lawful under (a) the GDPR, and (b) the ePrivacy regulatory framework? After two invitation-only workshops run under Chatham House rules, where actual processing operations were discussed,61 and one public workshop[62] attended by fellow academics, DPAs' and NGOs' representatives,

our opinion was formulated (under the necessary disclaimers) towards the negative: No, operations as described are not lawful under applicable law.[63]

However, we were not happy with our reply. As academics we could identify two regulation policy problems that came up repeatedly during our research. First, the societal need for increasing, not decreasing, big data analytics operations. Modern life would be inconceivable without the services afforded by electronic communications; none of them would be possible without some type of big data analytics run in the background. On top of that, public administrations were added to users while asking for ever-increasing processing capabilities: apart from enhancing the user experience while also keeping costs reasonable, electronic communications actors now also have to satisfy governments, who have been increasingly submitting big data analytics requests as an indispensable tool while drafting their public policies.

The second regulation policy problem pertained to the difference of approaches to big data analytics between the GDPR and ePrivacy laws. While the GDPR adopts a more nuanced approach, with flexibility filters evenly distributed in its text, the ePrivacy framework adopts a more rigid approach, abolishing exactly these GDPR flexibility filters. To make things worse, whatever effort the ePrivacy Directive made back in 2009 for a more layered approach, as demonstrated above in Sections 2 and 7, was completely abandoned, rather than expanded, in 2017 in the draft ePrivacy Regulation text.

Overall, therefore, the draft ePrivacy Regulation failed our law-making expectations in two ways. First, it failed to identify and regulate a social need: big data analytics by its addressees (telecommunications operators and internet service providers) is mandated, if not by market reality, then most definitely by public expectations and better-government needs. It therefore is in need of better regulation, not outright prohibition.

Our second law-making expectation that the draft ePrivacy Regulation failed to meet was the need for specificity. By now its addressees are not a handful of telecommunications operators but also all internet companies, thousands (if not millions) of enterprises of various sizes, business models, capitalisation and reach. We would have therefore expected at least an attempt by the legislator to distinguish and classify, to separate and specify. Telecommunications operators are not to be bundled together with internet companies, because they apply fundamentally different business models. Location data are not the same as traffic data, and each one differs substantially depending on who does the collection and processing. EPrivacy legislation needs to take all these into account and provide different, case-specific rules to each category of addressees. Instead, the draft ePrivacy Regulation took away even the modest attempt of the 2009 Directive to somehow distinguish within the field.

The mid-2019 elections offer a good opportunity to pause and think back; the ePrivacy Directive, combined with the Electronic Communications Code, provides a reasonable interim framework to work with for the near future, of course under GDPR supervision, as prescribed by the EDPB; and, the GDPR consistency and one-stop-shop mechanisms can address any claims for harmonised regulation across the EU.

A basic realisation, and at the same time a critical disclaimer of our paper, is that an ePrivacy Regulation regulates much more than big data analytics operations run by its addressees. Being a privacy and communication secrecy and not exclusively a data protection instrument it also deals with issues of confidentiality of communications, consumer law, internet cookies etc. Overall, therefore, an ePrivacy Regulation is indeed necessary. We therefore fully endorse the EDPS' prompt to "keep our eyes on the prize": indeed, the ePrivacy Regulation must not lower the level of protection foreseen in the GDPR.[64]

However, we believe that in order for the ePrivacy Regulation to accomplish its mission a much better law-making job needs to be done as regards the level of specificity its provisions need to reach. The EDPS is correct to state that not all issues are controversial and that compromises that ensure the necessary protection of fundament rights can be struck. We think, however, that this cannot be accomplished under the current draft, because, simply put, in treating all actors and all data in bulk it cannot find common grounds with anyone.

At the point of drafting this paper three future scenarios appear possible: first that the ePrivacy Regulation is voted in more or less its current wording. Second, that it is abandoned, and the GDPR is called upon to cover any regulatory gap. Third, that the ePrivacy Regulation is amended to meet the challenges discussed above. We believe that the first scenario, although most plausible to take place, will ultimately carry little, if any, added value to the electronic communications field, at least from a data protection point of view. If the ePrivacy legal framework is to meet its aims and purposes its provisions will have to be much more granular than the ones included in the draft ePrivacy Regulation. Its text will have to be much more detailed and technical, taking into account the different types of actors and purposes and the different types of personal data each one of them processes. Scalability can only be achieved through granularity.

The second and third scenarios are complementary, and, we believe, more suitable for the ePrivacy field. We suggest that the current draft ePrivacy Regulation be withdrawn and thoroughly revised, at least from a data protection point of view. In the meantime, the GDPR could hold the role of the rules-setting text also for the electronic communications field, combined with the ePrivacy Directive as amended by the Electronic Communications Code. EDPB intervention, wherever needed, could address any difficulties (as is, after all, also expected to do under the new ePrivacy Regulation regime). These tools would provide the EU legislator

with the necessary time in order to devise and present a new, much more detailed and granular ePrivacy text in the future that would indeed take into account actual social and market circumstances while supporting and promoting the data protection aims and purposes.