What Does It Matter Who is Browsing?

ISP Liability and the Right to Anonymity

by **Ciarán Burke and Alexandra Molitorisová***

Abstract: Disputes concatenating privacy, speech and security through the right to anonymity are particularly hard cases to adjudicate. The traditional paradigm, according to which anonymity plays a double role – protecting fundamental rights, as well as potentially threatening them – continues to drive policies that, in turn, emphasise the risks and downplay the opportunities of anonymity in the online world. The content/metadata distinction is a residue of such ambiguous views, persistent in the Court of Justice of the European Union's (CJEU) approach towards the right to anonymity in ISP liability cases. The article initially explores the argumentative grounds behind the CJEU's recent McFadden judgment (part B). Against the backdrop of the theory of balancing of interests, this paper critically examines the Court's reductionist position. Our critique suggests a method of avoiding the disproportionately narrow scope of analysis that accompanies this position. For this purpose, we establish the right to anonymity at the periphery of both the freedom of expression and information, and the right to private life and data protection, while contesting the right to anonymity as a right sui generis. We proceed with three key points. By inspecting the nature of the right to anonymity, we unveil the interconnectedness between the right to freedom of expression and information and the right to private life and data protection (part C). Chilling effects represent an often understated evidence of this relationship. In addition, we see that affecting certain means of exercising a particular fundamental right, such as is its anonymous exercise, brings forward important extra-legal considerations, facilitating the discernment of chilling effects in any analysis of human rights. It is argued that regulating anonymity could pose a significant obstacle to the exercise of a fundamental right as a whole, and consequently impact upon the core of that right (part D). Harmonisation-driven attempts to develop human rights guarantees, framed in seemingly robust procedures established by the CJEU, at the level of data collection or retention as well as data disclosure by an ISP, have the potential to be derailed by nation-specific considerations. Taking such considerations seriously can reverse the imminent impact upon the core of the fundamental rights in question, which the narrow scope of traditional human rights analysis easily discounts. This requires diverting from the "targeting by dissuasion" argument as a mere technical exercise, and acknowledging the subtle subterranean relationship of the fundamental rights being considered (part E).

Keywords: ISP liability; right to anonymity; Mc Fadden; chilling effects; fundamental rights; privacy; CJEU

Recommended citation: Ciarán Burke and Alexandra Molitorisová, What Does It Matter Who is Browsing? ISP Liability and the Right to Anonymity, 8 (2017) JIPITEC 238 para 1.

A. Anonymity: Disguised in Crowds and Technology

1 Let us briefly look back through the lens of history:

2 Ceausescu fell from power on 21 December 1989. In the last moment of his rule, to demonstrate the regime's lasting grip over the nation, the party's apparatus held a rally counting 80,000 people in the streets of Bucharest. Romanian citizens were instructed to pause their work and tune in the parade on their radios and televisions. Ceausescu appeared on the balcony at the headquarters of the Romanian Communist Party and overlooked the crowds. He praised the success of the Romanian socialism, and promised raising social benefits. "I want to thank the initiators and organisers of this great event in Bucharest, considering it is a...", he never finished his sentence. Eight minutes after the speech commenced, a person booed in the crowd and sparked the resistance of nearby bystanders as well as thousands of people sitting at the radios and televisions in what came down in history as the Romanian revolution. Until today, that person remains unidentified.[1]

3 Between 19 and 21 October 1905, uncontrollable violence spread over the city of Odessa. In the wake of the October Manifesto, and anti-imperialist propaganda flooding Russian cities, violent clashes with the Jewish population engulfed the city. For many involved, the cause of the Russian decline preceding these turbulent events became instantaneously self-evident and needed to be eradicated. Around 400 Jewish perished in the hands of unnamed crowds in just two days. A number of police and military officers benefited from the anonymity conveyed by pogroms, and disguised in civilian clothes participated in the massacre, instead of maintaining law and order. Likely, the perpetrators of these atrocities will never be identified.

4 Although the above examples demonstrate that the question of anonymity has long been considered both crucial and contested in terms of ensuring both societal order and individual liberty, this paper aims to add a contemporary perspective to the debate concerning the frictional relationship between anonymity and the protection of fundamental rights and freedoms. Such an intervention is warranted by the seemingly novel, but perhaps quite analogous, circumstances of modern society: online anonymity, enabled by technological advancements and endorsed by billions of indistinguishable Internet users, provides for similar risks and opportunities. On the one hand, anonymity diminishes accountability: it gives "license" to depart from the limits of legality in the sense of positive law, and permits individuals to escape accountability for the possible ramifications of their actions. On the other hand, anonymity empowers individuals in terms of their autonomy and personhood,[2] and protects them from unjustified interference with certain fundamental rights. Human experience has shown on countless occasions that an additional "shield" reinforcing the freedom of expression, such as a speech act made in anonymity, can be of existential importance to its exercise. If history is characterised by a continuous narrative of civilisation, anonymity, in turn, becomes instrumental, so that marginal discourses are not excluded from the conversation. This is often the case with regard to the expression of ideas that offend, shock or disturb, and call for more protection than information and ideas that are favourably received.[3] Since the Internet has now become one of the principal means by which individuals exercise their right to freedom of expression, enabling participation in political and societal activities and discussions, even a minor disruption within the Internet's architecture bears the risk of significant collateral damage.[4] Recalling the real-world situations of political expression of the past essentially brings the problem closer to the everyday experience of today: pervading online real-name policies attach identity more strongly (visibly and permanently) to every act of online expression than almost any real-world situation has ever done before;[5] and available technologies significantly facilitate the ways in which one's identity can be revealed,[6] such as data mining. A modern judge adjudicating hard cases at the intersection of privacy, speech, and security must thus become increasingly aware of the importance of users'

* Prof. Dr. Ciarán Burke is a Professor of International Law, Friedrich Schiller University Jena, Germany, ciaran.burke@eui.eu.

Mgr. Alexandra Molitorisová is a Research Assistant to Prof. Dr. Ciarán Burke, Friedrich Schiller University Jena, Germany, alex.molitorisova@gmail.com.

1 Harari, Y. N., Homo Deus: A Brief History of Tomorrow, Harvill Secker London, 2016, pp. 135-137.

2 Moyakine E., Online Anonymity in the Modern Digital Age: Quest for a Legal Right, Journal of Information, Rights, Policy and Practice, Vol 1, No 1 (2016), p. 4.

3 Handyside v United Kingdom, Merits, App No 5493/72, A/24, [1976] ECHR 5, (1976) 1 EHRR 737, (1979) 1 EHRR 737, IHRL 14 (ECHR 1976), 7th December 1976, ECtHR, para 49.

4 Ahmet Yildirim v Turkey, Merits, App No 3111/10, 18th December 1976, Second Section, ECtHR para 54.

5 Madrigal A., Why Facebook and Google's Concept of 'Real Names' Is Revolutionary, in The Atlantis, 5 August 2011, available at: <https://www.theatlantic.com/technology/archive/2011/08/why-facebook-and-googles-concept-of-real-names-is-revolutionary/243171/> (accessed on 10 March 2017).

6 Zingales N., Virtues and perils of anonymity: should intermediaries bear the burden?, TILEC Discussion Paper, DP 2014-025, July 2014, available at: <http://ssrn.com/abstract=2463564> (accessed on 10 March 2017).

individual preferences regarding identity disclosure when they exercise their freedom of expression.[7] At the same time, acknowledging the importance of anonymity and confidentiality on the Internet must not lead the same modern judge to refuse to protect the rights of others.[8] We will show in our account that in adjudicating the hard cases, it is especially his or her local knowledge of users, their preferences and behaviour, and possible causes of chilling effects in the local environment, that would have a particularly instructive force in the analysis.

5 The right to data protection and the right to private life benefit from anonymous exercise on similar terms. The anonymization of data provides for the ultimate protection of an individual, in the sense that anonymised data are not considered personal data as long as the data subject is not identifiable. Processing anonymized data can, in theory, never violate subject's right to privacy. Per Article 32(1)(a) of the General Data Protection Regulation (GDPR), anonymization (or pseudonymization) of personal data is considered necessary for ensuring data security when such data processing, in accordance with Article 6(1)(f) GDPR, is of legitimate interest to a controller.[9] Anonymization is further not only required under the current Directive 2002/58/EC on privacy and electronic communications as a *lex specialis* (E-Privacy Directive) with regard to traffic data (e.g. routing, duration of communication, location of terminal equipment, IP address), but is also explicitly upheld in Recital 9 of Directive 95/46/EC on the protection of individuals with regard to the processing of personal data (DPD) as a measure minimising the risks associated with data processing.

6 In order to contextualise criticism of the right to anonymity in legal terms, the dual character of anonymity must be further stressed throughout the article, as a grey zone between illegality and legality, as a tenet of protected fundamental rights, as well as a potential source of interference with other fundamental rights, which renders any kind of conflict involving a purported right to anonymity especially difficult to balance. For the purposes of understanding anonymity deontologically in online communication networks, we should consider the right to anonymity particularly with respect to two fundamental rights; namely, the right to private life and protection of personal data (Articles 7 and 8 of the Charter and Article 8 of the ECHR, with the latter conceived of solely as a right to privacy), and the right to freedom of expression and information (Article 10 ECHR, Article 19 UDHR, Article 11 of the Charter).

7 The right to anonymity was once again contemplated at the highest level of the European judiciary structure. In its recent judgment,[10] the Court of Justice of the European Union (CJEU or Court) concluded that Article 12(1) and (3) of Directive 2000/31 (the E-Commerce Directive) and Directives 2001/29 and 2004/48 did not preclude the grant of an injunction, requiring a provider of access to a communication network allowing the public to connect to the Internet to take a measure consisting in password-protecting the Internet connection, provided that users were required to reveal their identity in order to obtain a password and could not therefore act anonymously, so to prevent third parties from making a particular copyright-protected work available to the general public. In its analysis, the CJEU refrained from even briefly considering the protection of personal data. The balancing of interests test exclusively concerned the right to property versus the right to conduct business and the right to freedom of information. For the purposes of this article, the *Mc Fadden* judgment serves as a *point de départ* towards a critical assessment of the CJEU's piecemeal approach in adjudicating the right to anonymity. The critical analysis shows that framing matters. The way in which the right to anonymity is shaped, differs when considered in what we call pure data protection cases (recently, e.g. in *re Breyer* and *Tele2*), and when balanced against other rights in mixed cases, in which the frame of adjudication is dictated by these other rights (e.g. in IP and ISP liability cases, in *re Promusicae* and *Scarlet Extended*). This article does not plan to defend the right to anonymity. It rather reveals that, while being unable to outlaw anonymity as such on the one hand, and facing increasing difficulties in justifying certain indiscriminate identification measures on the other, the Court engages in soft behavioural techniques of effectively nudging (incentivising) users out of the anonymous space, so as to eliminate the risky grey zone in which anonymous Internet users operate. Marginally, it also points to a differentiation between users' content and metadata, and to the fact that while this differentiation is becoming less and less visible in data protection cases, its remnants retain a certain degree of relevance in mixed cases where the risks accompanying anonymity arise.

7 Delfi v Estonia, Merits, App No 64569/09, Chamber Judgment [2013] ECHR 941, 10th October 2013, ECtHR, para 92.

8 Ibid.

9 Esayas S. Y., The role of anonymisation and pseudonymisation under the EU data privacy rules: beyond the 'all or nothing' approach, in European Journal of Law and Technology, Vol 6, No 2, 2015.

10 Judgment of the Court (Third Chamber) of 15 September 2016, Tobias Mc Fadden v Sony Music Entertainment Germany GmbH, C-484/14, ECLI:EU:C:2016:68.

B. Anonymity as Privacy in the Mc Fadden Judgment

8 The *Mc Fadden* case represents a recent example of a mixed case – a category of disputes in which the right to privacy is invoked in the context of a litigation concerning another fundamental right (here, the right to property). Specifically, Sony Music asserted that its rights were infringed when its copyright protected work was made available on the Internet to the general public by means of a Wi-Fi network owned by Mr. Mc Fadden. Mr Mc Fadden was an entrepreneur, who facilitated anonymous access to that network free of charge as part of his marketing activities. In *re Mc Fadden*, the Court avoided answering, or even indicating, what broader societal ramifications the proposed measure could provoke. However, the fact that the right to data protection and the right to private life of Internet users were absent in the balancing of interests test[11] did not pass unnoticed.[12] The injunction imposed upon an ISP consisting of the mandatory identification of all of a network's users can unquestionably eliminate users' anonymity. In that regard, AG Szpunar posited that the obligation to register users and retain their data is clearly disproportionate to the pursued goal – securing the legitimate interests of third parties – and that the means selected provoke serious reservations concerning the protection of the right to privacy and the confidentiality of communications.[13] Similar arguments are echoed by a number of commentators,[14] and the authors of this article, too, sympathise with these calls for caution. However, in order to expose the convoluted relationship of the right to privacy and the right to freedom of expression and information through the right to anonymity, we propose that we should not rush to decide that the judges' reasoning is based upon an erroneous worldview or that it represents a technical error.[15] As a starting premise, we intend to accept that, in this case, societal concerns can be given their due weight in the balancing of legitimate interests, without explicitly weighting the right to privacy. This will aid in illustrating that while facing persistent criticism of playing a "catch me if you can" game with technological advancements, regulating the online environment involves exploring interdependencies of privacy, speech and security as freedom mediators, in order to induce deliberate changes in a decision context, minimising the risk of human behaviour.[16]

9 Primarily, two legal bases could be considered in parallel to ensure that such an identification measure – as proposed by the Court – works in accordance with law: (a) consent of the data subject; and (b) compliance with obligations to which the data controller is subject. First, measures could be implemented in such a way as to ask an individual to provide consent to data processing in order to access the Internet. Such technical measures can, for instance, consist of real-name policy requirements or of verification via an e-mail address, Facebook account, ID card or telephone number. The Court implies that it is the right to *freedom of information* which is solely affected here.[17] If a data subject is not prepared to make this privacy trade-off, the right to freedom of expression and information would suffer considerably. As a general criticism, such framing appears excessively narrow, and the Court's reassurance that an open Wi-Fi connection constitutes only one of several means of accessing the Internet[18] is insufficient. In many people's perception, it would not be a stretch to say that a data subject is *coerced* into surrendering a part of his or her privacy in exchange for exercising freedom of information. However, if multiple options to access the Internet exist, this exchange remains completely voluntary, and thus, compatible with a legitimate ground for data processing (Article 7(a) DPD). Such a situation would resemble requiring prior consent for the storage of cookies (per Article 5(3) of the E-Privacy Directive), where, if not consented to, many websites, including search engines, remain inaccessible to the Internet users,[19] a practice widely tolerated by the European

11 Judgment in Mc Fadden, ECLI:EU:C:2016:68, para 90.

12 Husovec M., Holey Cap! CJEU Drills (Yet) Another Hole in the E-Commerce Directive's Safe Harbors Holey Cap!, Forthcoming, Journal of Intellectual Property Law & Practice (JIPLP), published as draft at <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2843816> (accessed on 15 March 2017).

13 Opinion of Advocate General Szpunar delivered on 16 March 2016, Mc Fadden, C-484/14, ECLI:EU:C:2016:170, para 146.

14 Cholasta R., Korbel F., CJEU's judgment is opening the way for limiting anonymous access to the Internet <http://www.lexology.com/library/detail.aspx?g=dc9449ea-046b-4292-8a9f-59bccdf37a32> (accessed on 15 March 2017) or Stalla-Bourdillon S., The CJEU rules on free access to wireless local area networks in McFadden: The last(?) shudder of Article 15 ECD, the vanishing of effective remedies, and a big farewell to free Wi-Fi!, available at <https://peepbeep.wordpress.com/2016/09/15/the-cjeu-rules-on-free-access-to-wireless-local-area-networks-in-mcfadden-the-last-shrudder-of-article-15-ecd-the-vanishing-of-effective-remedies-and-a-big-farewell-to-free-wi-fi/> (accessed on 28 July 2017).

15 For criticism of balancing test, see McFadden P. M., Balancing Test, Boston College of Law Review, Vol 29:585, May 1988, p. 644.

16 See in the context of German constitutional debate, Schweizer M, Nudging and the Principle of Proportionality, in Mathis K., Tor A. (eds.), Nudging, Possibilities, Limitations and Applications in European Law, Springer (2016), p. 114.

17 Judgment in Mc Fadden, ECLI:EU:C:2016:68, para 82 and 83.

18 Judgment in Mc Fadden, ECLI:EU:C:2016:68, para 92.

19 For some types of cookies the consent is not mandatory. Those cookies include any technical information or information necessary for the provision of services. Under the proposed Regulation on Privacy and Electronic

regulator. The decision whether or not this practice amounts to an interference with privacy rights, remains within the sole disposition of the decision maker.[20] Moreover, the DPD itself and national data protection laws based upon its transposition already balance the fundamental rights at stake,[21] and provide for mechanisms maintaining a certain equilibrium, by setting default data protection standards and safeguards.[22] Therefore, if the human rights dimension is to be addressed with precision, it may be useful to centre the analysis around the effects of such a measure on the right to freedom of information.[23]

10 Secondly, the injunction imposes a duty to process certain personal data on the part of the ISP. The ISP may choose not to provide a space for consent with data processing to its users. Consent is only one of several legal grounds for the processing of personal data, and it does not exclude the possibility that other legal grounds may be appropriate to consider in a given case.[24] In that instance, Article 7(c) DPD prescribes that if national law enables the imposition of a specific obligation (here, for example, storing users' IP addresses and external ports), the data processing can be said to be necessary for compliance with a legal obligation to which the controller is subject. An ISP is forced by law to implement certain identification measures, which triggers the scrutiny of its legitimate interests in the balancing test, especially the freedom to conduct business. The Court holds that where a measure consists of marginal changes to the exercise of the ISP's activity, such a measure does not impact upon the essence of this freedom,[25] even if the ISP cannot choose between multiple options to terminate or prevent infringement. Yet, noticeably, in *re UPC Telekabel,*[26] if that ISP is left with more than one technical means to comply with an injunction (in addition to identification measures, the Court could, for example, consider limiting the type of communication passing through the Wi-Fi network), a domestic court must be able to exercise a secondary judicial review of a measure imposed on or implemented by the ISP. This leaves the balancing test interestingly unsettled, because the proportionality of a particular technical measure is assessed by a national court only *a posteriori* and only incidentally, with likely diverging outcomes. In our opinion, *re Mc Fadden* could be read in a similar fashion. The domestic court should ascertain whether revealing a user's identity in order to obtain a password to access a communication network would prevent the users acting anonymously and dissuade them from infringing copyright via peer-to-peer platforms.[27] At its core, given the differences in the identification measures contemplated, the national judge is supposed to assess the effectiveness (or the proportionality) of the relevant measure. The Court suggests that the eradication of users' anonymity may ensure genuine protection of the fundamental rights at issue,[28] and the national judge shall, in his or her turn, consider whether a particular identification measure is indeed capable of achieving the stated aim.[29] This includes answering the question as to whether the implemented measure goes beyond what is strictly necessary. It seems that in the case, it is possible to pursue the second step of the proportionality analysis in the proceedings before the national court, ergo re-open the aspects of privacy protection, and in particular data retention, in the legal analysis. In the final part of the article, we propose a guideline by which a national judge can consider approaching this dimension and re-join the human rights analysis in his or her part.

11 In the proportionality analysis, the question of whether the measure is strictly targeted, and does not impact upon a fundamental right more than is necessary, is only answered vis-à-vis the right to freedom of information. No other rights are considered. This has much to do with the European courts' view of the role of the Internet as a facilitator of the dissemination of information,[30] which enhances new forms of social interaction and revolutionizes the public's access to news.[31] Therefore, the measure should, above all, not affect the possibility of Internet users to lawfully access information using the provider's services,[32] a goal which should, in principle, be satisfied by

Communications no consent will be required for non-privacy intrusive cookies (e.g. the history of shopping cart).

20 Article 29 Working Party, Opinion 15/2011 on the definition of consent (WP 187), 13 July 2011.

21 Notably, Recital 37 and Article 9 of the DPD.

22 Judgment of the Court of 6 November 2003, Bodil Lindqvist, C-101/01, ECLI:EU:C:2003:596, para 82.

23 To criticism of human rights inflation in the online environment, e.g. De Hert, P., Kloza, D., Internet (access) as a new fundamental right. Inflating the current rights framework?, European Journal of Law and Technology, Vol. 3. No. 3, 2012.

24 Article 29 Working Party, "Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC", WP 217, 9 April 2014.

25 Judgment in Mc Fadden, ECLI:EU:C:2016:68, para 91.

26 Judgement of the Court (Fourth Chamber) of 27 March 2014, UPC Telekabel Wien, Case C-314/12, ECLI:EU:C:2014:192, para 57.

27 Judgment in Mc Fadden, ECLI:EU:C:2016:68, at 96 and 10.

28 Ibid, at 101.

29 Husovec M., supra note xii.

30 Times Newspapers Limited v the United Kingdom, App Nos 3002/03 and 23676/03, [2009] EMLR 14, 10th March 2009, ECtHR, para 27.

31 Opinion of Advocate General Jääskinen delivered on 25 June 2013, Case C-131/12, Google Spain, ECLI:EU:C:2013:424, para 121.

32 Judgment in Mc Fadden, ECLI:EU:C:2016:68, para 93.

not terminating the connection or blocking any Internet site as a source of information.[33] The right to information carries the risk of sharing or allowing others to share proprietary material of a third party or information of personal character; therefore, it necessarily involves a risk of fundamental conflict with the right to property,[34] or the right to privacy. Such a conflict must be resolved in accordance with the idea of achieving a fair balance.[35] This requires, in essence, assessing the problem of necessity, which the Court epitomizes through the notion of a targeted measure. If a measure does not block the transmission of lawful communication (e.g. due to the implementation of a system that inadequately distinguishes between unlawful and lawful content), the requirement of a strictly targeted measure is fulfilled.[36] In view of the foregoing, the fact that the injunction does not restrict access to available online sources appears a critical point. The implementation of the identification measures can change many aspects of such service – from unprotected to protected, from secure to insecure, from anonymous to non-anonymous network – but does not block the transmission. One cannot know beforehand what a user's true preference is,[37] e.g. to log into an anonymous network. Each default situation carries the possibility of untargeted side effects,[38] excluding one group from the use of the network. There may be users who would, in principle, never log into an anonymous or public network. Therefore, reversal of the situations does not necessarily interfere with the user's freedom to choose (here, to use a particular service).[39] The injunction is supposed to fulfil a dissuasive function[40] of unlawful use of the provider's services, and the Court appears to suggest that only secure and non-anonymous networks target such illicit use, and *ergo*, are proportionate to the aim pursued. In so doing, the Court pre-arranges the ground for testing the basic proportionality (see above). The acceptance that dissuasion does not in principle interfere with the lawful user's autonomy of will could explain why the Court addressed only the right to freedom of information and the right to conduct a business. In our conclusion, we will debate how the lack of harmonisation concerning data disclosure rules and the dissuasive function, which the injunction assumes, leads the analysis to its denouement by a national court, possessing nation-specific information.

C. Privacy, Browsing and Chilling Effects

12 Outlining the arguments that we believe might underline the Court's reasoning, reveals one notable argumentative lacuna that draws us away from the reductionist position. This lacuna is found in the Court's failing to consider so-called chilling effects. The lacuna will have to be filled by the reasoning of a national judge. Chilling effects bring into the legal analysis what is, in part, an extra-legal consideration (the same way a lack of legal certainty,[41] extensive interpretation of derogations, or the severity of punishment[42] affect human behaviour), and can sometimes become more problematic from a human rights perspective than direct infringements or interferences. A deterrent effect manifests itself as a shared negative human feeling regarding the lawful exercise of a fundamental right and can amount to an unwarranted abrogation of that right, with respect to particular individuals, sensitive groups, or the general population.

13 Chilling effects only become visible if the analytical focus is detached from the direct unlawful interference[43] and the letter of law. This requires a deeper understanding of: (i) the (meta)normative dimension of the interdependence of the relevant fundamental rights; and (ii) psychological, sociological, economic, and other factors that can influence the factual exercise of a particular fundamental right. Any understanding of the interdependencies is subject to the scope of analysis – what rights a judge is prepared to consider. It is a problematic, often perilous, trait of the balancing test to rightly identify the competing interests, not only of the litigants themselves, but also the broader interests that the litigants represent[44] and those that

33 Ahmet Yıldırım v. Turkey, Cengiz, App No, ECtHR and Others v. Turkey, App No, ECtHR, and further in Judgment in Mc Fadden, ECLI:EU:C:2016:68, para 92.

34 See e.g. Ashby Donald et Autres c France, App No 36769/08, 10 January 2013, ECtHR.

35 Judgment in Mc Fadden, ECLI:EU:C:2016:68, para 98.

36 Judgement of the Court in UPC Telekabel Wien, ECLI:EU:C:2014:192, para 56, Judgment in Mc Fadden, ECLI:EU:C:2016:68, para 93, and similarly, from Judgment of the Court (Third Chamber) of 24 November 2011, Scarlet Extended, ECLI:EU:C:2011:771, C-70/10 para 52.

37 Schweizer M, supra note xvi, pp. 100-101.

38 Insecure public networks leave the Internet user to deal with several inherent risks (e.g. data theft), and discourage lawful exercise of the right to information.

39 Schweizer M., supra note xvi, pp. 100-101.

40 Judgement of the Court in UPC Telekabel Wien, ECLI:EU:C:2014:192, and Judgment in Mc Fadden, ECLI:EU:C:2016:68.

41 See Cumhuriyet Vakfı and Others v Turkey, App No 28255/07, 8th October 2013, ECtHR.

42 Mosley v the United Kingdom, App No 48009/08, 10th May 2011, ECtHR or Morice v. France [GC], App No 29369/10, ECHR 2015, ECtHR ("*where fines are concerned as a moderate type of sanction, it would not suffice to negate the risk of chilling effects on the freedom of expression*", para 176).

43 In this case, affecting the possibility of using the ISP's services to access information lawfully. See Judgment in Mc Fadden, ECLI:EU:C:2016:68, para 94.

44 McFadden P. M., supra note xv, p. 586.

they can further advocate. It does not always become explicit, which fundamental rights should be placed onto the balancing scale and weighed against each other; for instance, in *re Delfi v Estonia*, the landmark case concerning the role of the ISP in regulating anonymous speech on the Internet, the ECtHR did not deal with the ISPs' freedom to conduct business, or in *re Google Spain*, notoriously known as the "right to be forgotten" case, the CJEU did not refer to a publisher's right to freedom of expression,[45] and denied any particular weight to Google's freedom of entrepreneurship. Furthermore, as regards point (ii), the widely accepted understanding of law as a system of rules prescribing and governing human behaviour[46] reveals why such factors matter in the analytical discussion: if a person comports with one rule, however, simultaneously, his behaviour thwarts the anticipated objective pursued by a second rule, the contradiction demands a resolution. The more limited the scope of the analysis is, the more difficult it is to detect the relevant impact on the other, co-existent, legitimate objectives. Sometimes only first exploring the extra-legal considerations (societal dimensions) reveal what fundamental rights it is specifically germane to address.

14 The mutual interdependence of the right to freedom of expression and right to privacy has been recognised by a number of authorities.[47] Chilling effects constitute often-cited evidence of the existence of this relationship.[48] However, this has not been the case with regard to the right to information, to which the Court confines its ruling. By examining the content of this right, several issues come to the surface: (i) the right to information covers both the right to impart and receive information[49] (i.e. establishes a broad right to communication, both private and public); (ii) the right covers not only the information, but also the way in which the information is conveyed,[50] *ergo*, it covers all means of communication;[51] and (iii) the right to information must be understood as a pre-condition of exercising freedom of expression[52] in its narrow sense.[53] What is the connection with the right to privacy? First of all, as regards the right to data protection, it has the distinctive feature of being both technologically and contextually neutral,[54] it is applicable to personal data passing through all means of communication. Furthermore, it is clear that private communication is an inseparable component of the right to private life.[55] The extent of Article 7 of the Charter corresponds to Article 8 ECHR; however, the word "communication" replaced the word "correspondence", to cover the wide variety of means through which people nowadays communicate both privately and publically.[56] However, if Article 11 of the Charter makes an apparent distinction between "information" and "ideas", this differentiation makes it more difficult to accept that the chilling effects caused by an interference with the right to privacy could impact upon the right to information equally to the freedom of expression, conceived narrowly. If information, in contrast to ideas, bears the badge of being "impersonal", "factual", and supposedly "impartial", the fact that the exercise of the right to information can be chilled by such interference is easily discounted. However, such a description is detached from today's reality. In a world where users are stimulated to overshare their personal data[57] and where the expression of public statements and private sentiments passes through the same communication means, imparting information (even if directed to a restricted group of recipients) potentially encompasses enormous breadth. To illustrate this, let us consider a few examples. Two interpretations of a single fact may appear on social

45 Fomperosa Rivero Á., Right to Be Forgotten in the European Court of Justice Google Spain Case: The Right Balance of Privacy Rights, Procedure, and Extraterritoriality, Stanford-Vienna Transatlantic Technology Law Forum, European Union Law Working Papers, No 19, p. 21.

46 Kelsen H., General Theory of Law and State, translated by Wedberg A., Harvard University Press, 1945, p. 3.

47 See Scharsach and News Verlagsgesellschaft mbH. v Austria, App No 39394/98, ECHR 2003-XI, ECtHR, para 30. Also as Frank La Rue, former Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression stated in his 2013 Report to the Human Rights Council noted: "*Privacy and freedom of expression are interlinked and mutually dependent*".

48 E.g. seminal Schauer F., Fear, Risk, and the First Amendment: Unraveling the "Chilling Effect," 58 B.U. L. REV. 685, 730 (1978).

49 See Article 11(1) of the Charter.

50 See, i.a., Jersild v Denmark, App No 15890/89, 24th September 1994, ECtHR (GK), para 31; 24.2.1997, De Haes and Gijsels v Belgium, App No 19983/92, 29th March 2001, ECtHR, para 48; Thoma v Luxembourg, App No 38432/97, 12th September 2001, ECtHR para 45, Palomo Sánchez v Spain, App No 28.955/06, 28th October 2014, ECtHR, para 53.

51 Murat Vural v Turkey, App No 9540/07, 21st October 2014, ECtHR, para 52.

52 See Open Door and Dublin Well Woman v Ireland, App Nos 14234/88 u 14235/88, 29th October 1992, ECtHR.

53 Recommendation CM/Rec(2014)6 of the Committee of Ministers to member States on a guide to human rights for Internet users Explanatory Memorandum, available at: <https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016805c6f85>, p. 40 (accessed on 8 March 2017).

54 Lynskey O., Deconstructing data protection: the "added-value" of a right to data protection in the EU legal order, 63 International & Comparative Law Quarterly (2014), p. 577.

55 Article 7 of the Charter (Respect for private and family life) prescribes that everyone has the right to respect for his or her private and family life, home and *communications*.

56 Explanations relating to the Charter of Fundamental Rights. Official Journal of the European Union C 303/17 - 14.12.2007.

57 See Jozwiak M., Balancing the Rights to Data Protection and Freedom of Expression and Information by the Court of Justice of the European Union. The Vulnerability of Rights in an Online Context, 23 MJ 3 (2016), p. 419.

media accounts in the following manner:

a) One third of stock market inventors believe that at least one country will leave the Eurozone in the next 5 years;

b) Two-thirds of stock market investors believe that all Eurozone countries will stay in the monetary union for the next 5 years.

15 An individual's reaction to share (i.e. to immediately impart information that was just accessed) one of the two interpretations of a certain piece of information can depend on how that information is framed, and the preference to share one piece of information over another can reveal much about the individual's political stance. Two Google searches[58] could look like this:

a) Basic income doomed to fail;

b) Happy people; basic income; Finland.

16 Alternatively, two browsing paths could consist of the following steps/clicks:

a) Edward Snowden – Is Edward Snowden a Hero? – Bernie Sanders on the Exile of Snowden;

b) Edward Snowden – Is Edward Snowden a Hero or Traitor? - Obama Says Snowden is Not a Patriot.

17 The frame employed by a user, or the links the user clicks, can reveal much about his own interests, constituting a significant component of privacy. An aggregation of the imparted or accessed information can generate a representative overview of the individual's political and other opinions.[59] The right to freedom of expression is not more susceptible to be affected by the chilling effects prompted by lawful interferences with privacy than the 'mere' right to information. Although more empirical data is needed as regards users' browsing behaviour, similar observations were made with respect to decreasing traffic to or avoidance of several Wikipedia articles that raised privacy concerns in the post-Snowden era, such as those containing words like "jihad", "al-Qaeda", "suicide attack", "Islamist", or "Dirty Bomb".[60] Clearly, the ability to freely access information is as intrinsically linked to privacy as holding one's opinions and expressing them. As the freedom of expression and right to information are both indispensable for "uninhibited, robust, and wide-open"[61] debate and communication,[62] understanding that chilling effects can occur with respect to each right equally is essential for future analytical purposes. In order to ensure the human rights dimension of the online environment, the right to freedom of expression and information should not be arbitrarily separated. It is perhaps only encouraging that the CJEU is not always oblivious to potential behavioural effects that an interference with the right to privacy might provoke. In *DRI*, it noted that: "the fact that data are retained and subsequently used without the subscriber or registered user being informed is likely to generate in the minds of the persons concerned the feeling that their private lives are the subject of constant surveillance".[63] It remains germane to ask what primary interferences with the right to privacy may trigger these effects. In legal terms, does an entitlement to exercise a particular fundamental right anonymously exist, and if so, under what conditions may such an entitlement be abridged?

D. Anonymity on the Periphery of Fundamental Rights

18 In attempting to construct a permission to enjoy particular rights anonymously as a *right* to anonymity,[64] separable from the rights being enjoyed, one can be guided by the principle of equality before law. Fundamental rights stem from the doctrine of universality,[65] and are conferred upon *everyone* on a non-discriminatory basis, regardless of origin. Alternatively, the right to anonymity can be said to stem from the principle of personal autonomy,[66] as the ability to conduct one's life in a manner of one's choosing,[67] as well as the freedom to make decisions,

58 According to AG Jääskinen in Google Spain, ECLI:EU:C:2013:424, search processes constitute an important concretisation of the freedom of expression.

59 Ohm P., Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization, 57 UCLA Law Review 1701 (2010).

60 Penney J. W., Chilling Effects: Online Surveillance and Wikipedia Use, 31 Berkeley Tech. L.J. 117 (2016).

61 New York Times v Sullivan, 376 U.S. 967 84 S. Ct. 1130 12 L. Ed. 2d 83 1964 U.S., U.S. Supreme Court.

62 Wachter S., Privacy: Primus Inter Pares Privacy as a precondition for self-development, personal fulfilment and the free enjoyment of fundamental human rights, available at <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2903514> (accessed on 8 March 2017).

63 Judgment of the Court of 8 April 2014, Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, Commissioner of the Garda Síochána, C-293/12, ECLI:EU:C:2014:238, para 37.

64 Moyakine E, supra note ii.

65 Nickel, James. Making Sense of Human Rights: Philosophical Reflections on the Universal Declaration of Human Rights, (Berkeley; University of California Press, 1987), pp. 561-2.

66 *Per* AG Maduro's opinion in case C-303/06 S. Coleman v Attridge Law and Steve Law, on 31 January 2008, ECLI:EU:C:2008:61, personal autonomy and human dignity are values underlying the principle of equality, para 8.

67 Pretty v the United Kingdom, App No 2346/02, 29th April

the freedom to act (including contractual liberty),[68] the freedom to choose to be left alone,[69] or the *right* to establish details of one's identity as an individual human being.[70] It is a principle that underpins the interpretation of *all* guarantees of the ECHR.[71] However, both constructs appear challenging; first of all, the right to anonymity *per se* does not find its legal basis in the current *lex lata* – neither universality nor autonomy can be neatly reduced to anonymity. Secondly, there exists a strong dialectical relationship with a number of recognised fundamental rights (the right to assembly, freedom of religion, freedom of thought, freedom of expression and freedom of association); it stands in a position, from which it potentially overlaps with several of these rights simultaneously. Therefore, it is difficult to grant anonymity the benefit of a separate positive right *sui generis*. With this criticism in mind, it is proposed to view the right to anonymity as a right that potentially dwells within the penumbra of other rights. Several of the Court's judgments[72] as well as recent EU policy and legislative decisions and more traditional policies of the Member States endorsing real name identification requirements preclude a contrary view. These measures on the one hand, and advocating restrictive positions on the compulsory identification of users accessing the Internet or using encryption technologies on the other,[73] leave policy-makers with a complex political problem. Anonymity makes for a malleable phenomenon, the risks and benefits of which are, in turn, accentuated and depreciated vis-à-vis a particular policy objective. For example, the Commission's latest proposal to review the Anti-Money Laundering Directive avows that in the context of virtual currency markets, anonymity is rather a hindrance than an asset and calls for the identification of users of virtual exchange platforms and custodian wallet services.[74] A similar trend is indicated by the adoption of the Directive on the Passenger Name Record Data.[75] Also, traditionally, at the level of the Member States, mandatory identification measures relate to many private or public law areas such as hotel guest registration, company ownership, or real estate purchase publicity. On the other hand, concerns about de-anonymization and re-identification of data sources persist, and are considered a serious obstacle to an EU-wide data-driven economy.[76]

19 The core, as opposed to the penumbra, of a fundamental right, is generally constructed as an absolute limit to balancing.[77] It customarily refers to certain important elements[78] that together constitute the very substance of the right.[79] If the core of a fundamental right is to be preserved, the balancing test should not touch upon these elements. However, the situation with the right to data protection and right to private life is rather more entangled. One can sense a certain paradox in stating that a freedom to choose whether to be identifiable, identified or to remain in anonymity, does not constitute the core of the right to privacy, notably if one concedes that: (i) anonymization is the strongest form of data protection (anonymised data are not considered personal data); and (ii) Article 7 of the Charter centres around personal autonomy,[80] i.e.

2002, ECtHR, para 62.

68 Judgment of the Court of 5 October 1999, Kingdom of Spain v Commission of the European Communities, Case C-240/97, ECLI:EU:C:1999:479, para 99.

69 See Marshall J., Personal Freedom through Human Rights Law? Autonomy, Identity and Integrity under the European Convention on Human Rights, Martinus Nijhoff Publishers, Leiden, 2009.

70 Goodwin v the United Kingdom, App No 28957/95, 11th July 2002, ECtHR (GC), para 90.

71 Ibid.

72 E.g. Judgment of the Court of 19 October 2016, Case C-582/14, Patrick Breyer v Bundesrepublik Deutschland, ECLI:EU:C:2016:779 and Judgment in Mc Fadden, ECLI:EU:C:2016:68.

73 See e.g. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, available at: <http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf>, pp. 88 and 89 (accessed on 7 March 2017).

74 Proposal for a Directive of the European Parliament and of the Council amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and amending Directive 2009/101/EC (COM(2016) 450 final).

75 Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime.

76 EPSC Strategic Notes, 11 January 2017, available at: <https://ec.europa.eu/epsc/sites/epsc/files/strategic_note_issue_21.pdf> (accessed on 6 March 2017).

77 von Bogdandy A., Kottman M., Antpöhler C., Dickschen J., Hentrei S., et altri, Reverse Solange – Protecting the Essence of Fundamental Rights against EU Member States, Common Market Law Review, 49.2 (Apr 2012), pp. 489 to 519.

78 On the essence of fundamental rights, see Brkan M., In search of the concept of essence of EU fundamental rights through the prism of data privacy, Maastricht Faculty of Law Working Paper 2017-01, pp. 13 to 15.

79 There are instances when the Court interpret the core of a fundamental right as a very possibility of exercising of the right ("*being carried out as such*", in Judgment of the Court of 20 May 2003 Österreichischer Rundfunk u.a., C-465/00, ECLI:EU:C:2003:294, at 49). Nonetheless, at other instances, the court avows that if the wording of the Charter does not suggest that the right is inviolable (such as in contrast the right to life), there is no reason that to absolutely protect such a right (Judgment of the Court of 16 February 2012, SABAM, C-360/10, ECLI:EU:C:2003:294, at 41). Also, similarly to Article 17 ECHR, which states that the ECHR may not "*be interpreted as implying for any State, group or person any right to engage in any activity or perform any act aimed at the destruction of any of the rights and freedoms set forth herein*."

80 See Commentary of the Charter of Fundamental Rights of the European Union. ECtHR too places personal autonomy

freedom *largo sensu*, including making decision about whether to remain anonymous or what information concerning an individual should be anonymised. However, these points appear mutually self-reinforcing, and if they should validate the position of the right to anonymity within the core of the right to privacy, the tautology would deprive the latter of any specific essence or periphery with respect to data protection (*a contrario* to Article 52(1) of the Charter, and *ad absurdum* all personal data could belong to the core of the right to privacy and any de-anonymization of any data would violate the core of the right). The Court's earlier jurisprudence suggests that the object of the right to privacy is, *inter alia*, a bundle of personal data, of which some belong to its core and some do not. Both rulings in *res DRI* and *Schrems*[81] upheld the classic metadata/content distinction. Balancing *per* Article 8(2) of the Charter, guided by the Member States' discretion (Article 5(2) DPD),[82] could determine which data belongs to which category. An individualised approach is required,[83] while in particular, data sensitivity and the public interest in obtaining specific information must be taken into account.[84] In this respect, the essence of the right to private life has, *inter alia*, been found in the impermissibility of such derogations and limitations to the protection of personal data that would allow for accessing the *content* of electronic communications on a generalised basis in light of the objective of securing public protection.[85] More recent judgements, however, seem to depart from this position. The Court started to recognise that just because particular data processing concerns metadata (such as the name or IP address of a user, information on the periphery of the right to privacy) as opposed to content, it cannot be automatically concluded that such processing is permissible.[86] In *re Tele2*, the Court noted that the relationship could be far more complicated and meaningful. This accompanied a realisation of the potential for data identification that is accessible in today's Internet architecture (*re Breyer*). If ISPs are required to trace and identify the source of a communication and its destination, to identify the date, time, duration and type of a communication, to identify users' communication equipment and its location, the retained data has the potential to describe with precision the private life of individuals concerned ("everyday habits, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them").[87] It follows that metadata, or at least in bulk, is no less sensitive than the actual content of communications.[88] As such, it is the authors' view that the core or periphery of the right to privacy can be determined upon evaluation of the relationship between nature of the information relating to a person and the exercise of that person's autonomy in relation to that information.

20 In *re Coleman*, AG Maduro posited that the value of personal autonomy (underlying the principle of equality) dictates that "individuals should be able to design and conduct the course of their lives through a succession of choices among different valuable options". As such, the exercise of autonomy requires an array of relevant options from which to choose.[89] To be anonymous is certainly an expression of personal autonomy; it is a *means* of exercising a particular fundamental right. Indeed, there are other (equivalent) *means* of such exercise, each arising from the personal autonomy of individuals and protected under the principle of equality, unless such would amount to an abuse of law or would constitute an interference with other fundamental rights. The word "*means*" is key here. Means do not operate alone, but their character and importance must be determined with regard to upon what actions or information they are exercised. Any such *means*, expressions of autonomy, including

under the scope of the right to privacy *per* Article 8 ECHR (Kalacheva v. Russia, App No 3451/05, 7th May 2009, Tysiac v Poland, App No 5410/03, 20th March 2007, para 107 or Munjaz v the UK, App No 2913/06, 17th July 2012, para 80).

81 For a long time, other scholars have argued that systematic collection of traffic data affects the inviolable core of the right to privacy (e.g. LIBE Committee Inquiry on Electronic Mass Surveillance of EU Citizens Hearing, European Parliament, 14 October 2013, Statement by Professor Martin Scheinin (EUI), former UN Special Rapporteur on human rights and counter-terrorism).

82 See e.g Judgement of the Court of 29 January 2008, Promusicae, Case C-275/06, ECLI:EU:C:2008:54, para 70. The Court insisted on the need to interpret the DPD and E-Privacy Directive so as to allow a fair balance to be struck between the various fundamental rights protected by the EU legal order.

83 Judgment of the Court of 24 November 2011, ASNEF, Cases C-468/10 and C-469/10, ECLI:EU:C:2011:777, para 47.

84 Judgement of the Court (Grand Chamber) of 13 May 2014, Google Spain, C-131/12, ECLI:EU:C:2014:317, para 81 and similarly Delfi v Estonia, App No 64569/09, 16 June 2015, ECtHR, para 132 and Opinion of AG Bobek, delivered on 26 January 2017, C-13/16, Rīgas satiksme, ECLI:EU:C:2017:43, para 69.

85 Judgment of the Court (Grand Chamber) of 6 October 2015, Schrems, C-362/14, ECLI:EU:C:2015:650, at 94.

86 Also, in the words of ECtHR: *"[A]lthough freedom of expression and confidentiality of communications are primary considerations and users of telecommunications and Internet services must have a guarantee that their own privacy and freedom of expression will be respected, such guarantee cannot be absolute and must yield on occasion to other legitimate imperatives, such as the prevention of disorder or crime or the protection of the rights and freedoms of others."* K.U v Finland, App No 2872/02, 2nd December 2008, ECtHR, para 49.

87 Judgment in Tele2 Sverige, ECLI:EU:C:2016:970, para 98 and 99.

88 Ibid.

89 Opinion of AG Maduro in Coleman, ECLI:EU:C:2008:61, para 9.

anonymity, could be then found on the periphery of a fundamental right. However admittedly, interfering with some *means* could pose a significant obstacle to the exercise of a fundamental right as a whole, and consequently impact upon the core of that right. To verify the impact, the wording of Article 52(1) of the Charter would dictate that any limitation, for example, of the right to anonymity, must be provided for by law, be proportionate, necessary and genuine objectives of general interest recognised by the EU or by the need to protect the rights and freedoms of others.[90] In this sense, the autonomy of some could trump the autonomy of others (as was the case, for example, in *re Österreichischer Rundfunk*, where it was held that public access to information must be accorded priority over contractual freedom,[91] or in *re Google Spain*, where it was held that the data subject's rights override, as a general rule, the interest of Internet users to access information).

21 Is it important to weigh the right to anonymity separately as a tenet of the right to privacy in any human rights analysis concerning anonymity? Yes. Such analysis helps us to reveal the relationship between the identification data and other information at issue, some of which could belong to the core of the right to privacy. This could also clarify the significance of the data at issue in respect to other fundamental rights (for example, the freedom of expression). EU law is sometimes explicit about the relationship: processing of personal data under Article 8 DPD (e.g., concerning political opinions, religious or philosophical beliefs), represents the only data processing that a Member State is allowed to exclude in a categorical and generalised manner, without the need to balance competing interests.[92] Personal data under Article 8 DPD can be processed only consensually or anonymously. This also has consequences for the right to freedom of expression. Political expression of any kind and debate of public interest benefit from the widest protection; there is very little room left to justify restrictions on political expression, unless the latter amounts to incitement to violence.[93] Nonetheless, to establish the existence of an interference with the right to privacy, it does not matter whether the information in question is sensitive.[94] Such interdependences explain why the chilling effects on the exercise of the right to freedom of expression and information (occurring through the interference with the right to privacy) only become relevant to consider when both rights are present in the analysis. If the balancing test is concerned exclusively with the primary infringements of the right to privacy, and the right to freedom of expression and information does not directly suffer, the chilling effects remain indiscernible in the analysis (e.g. in case of surveillance). *A contrario*, if the primary infringement only affects the right to freedom of expression and information, the subtle role of personal autonomy (understood as a tenet of the right to privacy) risks to stay unappreciated. This poses legal dilemmas, especially in the adjudication of ISP liability cases, where additional fundamental rights must be factored into the balance (usually the freedom to conduct a business per Article 16 of the Charter, the right to property including IP, protected by Article 17 of the Charter, and the right to a remedy guaranteed by Article 47). Juggling three or more fundamental rights simultaneously requires a robust methodology, or it may risk overlooking a particular two-sided balance.[95] Although weighing several competing interests gives the state the benefit of a wide margin of appreciation,[96] the mechanism of fair balancing must be carried out individually, on the basis of a context-dependent analysis.[97] In this respect, the Court's case law has proceeded with interesting evolutionary dynamics. In our account, the dynamics can be epitomised by the following phases:

22 (i) first, the Court established the legal framework for the imposition of an injunction *per* Article 11 of Directive 2004/48. Following this framework, as a measure designed by national law, in light of the principle of proportionality, and within the prescribed confines (Article 6 and 15(1) of the E-Commerce Directive, Article 2(3) and 3 of Directive 2004/48) must be effective and dissuasive in nature.[98] The *e-Bay* ruling, above all, modelled a particular procedure for complex balancing, which allows for factoring many conflicting interests and fundamental rights into ISP liability cases;[99]

23 (ii) the Court subsequently rejected injunctions, which involve measures combining systematic *content* analysis and processing of information connected with users' profiles[100] or IP addresses,[101]

90 Judgment of the Court (Grand Chamber) of 21 December 2016, Tele2 Sverige, C-203/15, ECLI:EU:C:2016:970, para 94.

91 Judgment of the Court in Österreichischer Rundfunk u.a., ECLI:EU:C:2003:294, para 66.

92 Judgment of the Court in ASNEF, ECLI:EU:C:2011:777, para 48.

93 Joined App No 23927/94 and 24277/94, Sürekand Özdemir v. Turkey, 8 July 1999, ECtHR (GC), para 46.

94 Judgment of the Court in Schrems, ECLI:EU:C:2015:650, para 89.

95 Judgment of the Court in Promusicae, ECLI:EU:C:2008:54, para 65 and 66, and Judgment of the Court in Lindqvist, ECLI:EU:C:2003:596, para 85.

96 Neij and Sunde Kolmisoppi v Sweden, App No 40397/12, 19th Febraury 2013, ECtHR, part D.

97 See supra note lxxxv.

98 Judgement of the Court of 12 July 2011, L'Oréal, C-324/09, ECLI:EU:C:2011:474, para 135, 136 and 144.

99 Also see similarly K.U v Finland App No 2872/02, as discussed in Zingales N, supra note vi, p. 20.

100 Judgment of the Court in SABAM, ECLI:EU:C:2003:294, para 49.

101 Judgment of the Court in Scarlet Extended,

i.e. personal data which, in principle, allows those users to be identified;[102]

24 (iii) thirdly, the Court emphasised that a targeted injunction must seriously discourage only illicit behaviour. An example would be a prohibition imposed on an ISP to allow users to access a particular website.[103] The reasoning of the Court gives the impression that the Court does not prescribe that casting such an injunction must entail consideration of the right to privacy by default;[104]

25 (iv) finally, the Court held an injunction permissible, which dissuades the users from wrongdoing by identifying them.[105] As follows from (ii) and (iii), such a measure is targeted, if no communication content is directly analysed or blanketly monitored by an ISP. Again, in this instance users' interest in privacy has not been taken into account.

26 These phases indicate that ISP liability cases continue to be pre-occupied with the "old" content/metadata differentiation, making it relatively easier for a judge to place a final relational operator within the confines of the balancing test. Disabling anonymity certainly represents a viable alternative to enhanced content monitoring,[106] and as such, can eliminate certain doctrinal troubles with human rights dimensions. However, if a judge pursues the analysis through the unbecoming content/metadata dichotomy, and starts considering metadata (identification data) as something "merely" on the periphery of the fundamental rights, he or she becomes less concerned with the potential risk of neglecting related privacy and autonomy issues in a given case. There is a subsequent danger that the scope of the court's analysis is disproportionately narrow.

E. ISPs, the Identification Potential of Data and Data Disclosure

27 Historical experience has confirmed on numerous occasions that if a bearer of fundamental rights fears the legal, societal, or other ramifications of an exercise of these rights, he may find himself taking part in an uneasy decision between self-incrimination and self-censorship.[107] In other words, the right holder suffers from a chilling effect. In legal terms, a bearer of fundamental rights exercising this right within the confines of the law, may fear that the effect of such an exercise might either result in discrimination[108] or arbitrariness on the part of law enforcement. From the human rights perspective, it should in principle not matter whether chilling effects constitute a long-term phenomenon or, as certain research suggests, that this effect may fade away due to a growing insensitivity vis-à-vis a particular subject or practice.[109] Consensual data processing can mitigate the chilling effects to a certain extent; however, only if consent is informed and only if other equally valid choices are left for a decision maker (user) to take. Informed consent aims at eliminating an information asymmetry between a data controller and a data subject,[110] which means that the data subject should know when and to what data processing the consent is given, including an eventual data disclosure under national laws. At the same time, informed consent would not be enough if a data subject is deprived of valuable options (*means*) that would undercut his or her autonomy.[111]

28 To justify the interference with the right to information, the Court notes that a Wi-Fi network is only one of the possible ways to access the Internet. Nonetheless, in AG Szpunar's view, Wi-Fi networks are special in the sense that they offer "great potential for innovation".[112] It is therefore at least debatable whether an open public Wi-Fi or a home VDSL are equally valuable options for the exercise of the freedom of expression and information. Yet, if the main concern of personal data protection is a *large-scale* processing by mechanical, digital means, in all its varieties,[113] the analysis of the chilling effects should also be confined to this frame. Hence, while the *Mc Fadden* ruling and the national judgment that followed suit, thus far represent the only cases concerning such identification measures, the availability of choices (secured vs. unsecured networks) will eventually depend on how frequently copyright holders protect their rights via such

ECLI:EU:C:2011:771, para 51.

102 Supra note c.

103 Judgement of the Court in UPC Telekabel Wien, ECLI:EU:C:2014:192, para 42.

104 Ibid, para 47.

105 Judgment of the Court in Mc Fadden, ECLI:EU:C:2016:68.

106 Zingales N., Virtues and Perils of Anonymity Should Intermediaries Bear the Burden?, JIPITEC (2014), p. 162.

107 See also joint dissenting opinions of Judges Sajó and Tsotsoria in Delfi AS v Estonia, ECtHR judgment, notably para 3 and 14.

108 PEN's survey, Chilling Effects: NSA Surveillance Drives Writers to Self-Censor, 2013.

109 See Preibusch S., Privacy Behaviour After Snowden June Revelations, 58 Communications of the ACM.48; pp. 48-52 (2015).

110 Zuiderveen Borgesius, F. J., Improving privacy protection in the area of behavioural targeting (2014), available at: <https://pure.uva.nl/ws/files/2141324/154447_05.pdf> (accessed 15 April 2017).

111 Opinion of AG Maduro in Coleman, ECLI:EU:C:2008:61, para 11.

112 Opinion of AG Szpunar in Mc Fadden, ECLI:EU:C:2016:170, para 149.

113 Opinion of AG Bobek in Rīgas satiksme, ECLI:EU:C:2017:43, para 95.

means, and how many ISPs are forced to discontinue their services due to the costs of compliance with data protection requirements. The important implications of that are that a single infringement occurring within a particular communications network is sufficient enough to justify an injunction *per* Article 8(3) of Directive 2001/29, or Article 12(3), of the E-Commerce Directive.

29 However, from the perspective of chilling effects, it could appear more dangerous to impose an obligation upon an ISP to identify all of the network's users without the consent of the latter, following Article 7(c) DPD. For such an obligation to apply, it must be imposed by a law that unequivocally allows for its imposition and which, on its own, complies with data protection requirements, including the requirements of necessity, proportionality and purpose limitation.[114] Post *re Mc Fadden*, the proportionality of the legal obligation to collect and retain certain personal data must be tested by the judiciary, otherwise non-consensual automatic processing is inconceivable. The Court does not consider which data in particular should be collected and retained. As such, a question must be posed in relation to the principle of data minimisation *per* the DPD.[115] In this respect, it is important to note again that the contemplated identification measures should accomplish a dissuasive function. Dissuasion should be effective to such an extent as to ensure that fundamental rights would no longer be violated.[116] From the view of basic proportionality, this could only be done by requiring such identification data as would be strictly necessary for the purposes of initiating a judicial proceeding.[117] Only such identification measures, which substantially facilitate and enable the enforcement of infringed rights, would effectively dissuade potential infringers from future infringements. Because the data required to initiate court proceedings differs among the Member States, the national court must establish that the identification measure does not go beyond these data requirements. As such, assessing basic proportionality could be a mere technical issue, devoid of further judicial considerations. Further, it is important to note, as the Court did in *re Promusicae,* that the E-Privacy Directive, the E-Commerce Directive and Directives 2001/29/EC and 2004/48/EC do not oblige the Member States to impose an obligation to disclose in order to ensure effective protection of copyright. Hence, in the proportionality analysis, the obligation to identify Internet users, i.e. to collect and retain personal data, must be decoupled from the obligation to disclose, as a potential secondary legal obligation imposed upon an ISP.

30 Although the obligation of confidentiality of personal data can be restricted under the E-Privacy Directive for the protection of the rights and freedoms of others[118] (such as in the context of civil proceedings),[119] it is a matter of national law to provide a legal basis for a data disclosure.[120] In this framework, data disclosure[121] functions in the same manner as any other data processing; it must comply with the robust procedural scheme applicable to the obligation to process personal data in general. This means a fair balance must be struck[122] between multiple competing interests[123] by taking due account of the principle of proportionality. A fair balance cannot be struck, if a request for data disclosure is not substantiated and does not follow a legitimate interest. In addition to this, further safeguards must be provided: evidence of an infringement must clearly exist, information must be deemed important for the investigation, and due process must be guaranteed.[124] Undoubtedly, an interest of a (IP) right holder to sue an infringer for damages can be qualified as legitimate.[125] If a national law allows for data disclosure to protect right holders' interests in effective law enforcement, and such disclosure follows the prescribed procedural framework, which is appropriately balanced, EU law does not preclude such national legislation (*re Bonnier*). This multiple (though repetitive) procedural reasoning (at entry – data collection, data retention and at exit – data disclosure) should, in principle, guarantee that any interference with the right to privacy would bring a meaningful result after balancing. Nonetheless, if the effectiveness of identification measures is

114 Article 29 Working Party, "Opinion 15/2011 on the definition of consent" (WP 187), 13 July 2011.

115 Article 6(1)(c) and recital 28 of the DPD require that personal data must be adequate, relevant and not excessive in relation to the purposes for which they are collected, but also when further processed.

116 Judgment in Mc Fadden, ECLI:EU:C:2016:68.

117 In this regard, also Opinion of AG Bobek in Rīgas satiksme, ECLI:EU:C:2017:43, para 89.

118 Judgment of the Court in Promusicae, ECLI:EU:C:2008:54, para 53.

119 Ibid, para 54.

120 See also Zingales N., supra note cvi.

121 E.g. following an order served upon an ISP to give a copyright holder an information revealing identity of a particular subscriber (an alleged infringer) per Directive 2004/48, to whom the ISP provided an IP address. Judgment of the Court (Third Chamber) of 19 April 2012, Bonnier Audio and Others, C-461/10, ECLI:EU:C:2012:219, para 36.

122 Judgment of the Court in Bonnier Audio and Others, ECLI:EU:C:2012:219, para 60 and Order of the Court of 19 February 2009, LSG-Gesellschaft, C-557/07, para 29.

123 Judgment of the Court in Bonnier Audio in Others, ECLI:EU:C:2012:219, para 58.

124 Judgment of the Court in Promusicae, ECLI:EU:C:2008:54, para 70.

125 By analogy, Opinion of AG Bobek in Rīgas satiksme, ECLI:EU:C:2017:43, at 65. At the stage of initiating legal proceedings, "*[t]he disclosure in itself would therefore not even bring about any immediate change to the legal situation of the data subject*", para 81.

evaluated only on the basis of the inevitability of prosecution and punishment of infringement of third parties' rights, assessing basic proportionality, although repetitive, appears to be an *a priori* solved problem. Secondly, there is the problem of data retention period. The idea is that personal data should in principle not be retained for longer than necessary in relation to the purpose for which they were collected or for which they are further processed. The period for which personal data can be stored must be limited to a strict minimum, and systems should be designed by default to minimize the retention period of personal information (Recital 39 of the Preamble and Article 25 of the GDPR). If the purpose of the data processing is to deflect the users from potential wrongdoing, by giving an effective possibility of initiating criminal proceedings, then the data retention period should in theory last until time for such initiation objectively lapses under national law. The data retention period is not tailored in accordance to the severity of wrongdoing, if an objective limitation period applies. However, an obligation to disclose data is not limited to a particular type of wrongdoing – let's say copyright infringement. If the permissible data retention period is not proportionately limited to the severity of the wrongdoing, but it is set objectively in accordance with the dissuasive function of the injunction – as considered by the Court – there is a risk of unjustified interference with the right to data protection. In ten years' time, new technologies can make use of current data, mandatorily stored by and ISP, in a way no one can predict. Consider only that a few years ago, that facial recognition technology was in many ways a vision of a distant future. Today, for example, every photo ever stored on a social media platform has the potential to be used for face recognition purposes. Such foresight and risk assessment of potential data uses should appear in the balancing exercise.

31 If an ISP is served with an order to secure its network and national law provides for a duty to disclose identity in court proceedings, an ISP becomes a part of the law enforcement framework. Different injunctions can be served, requiring the processing of different personal data with respect to different ISPs,[126] together making it reasonably easy to establish "the author of the crime" in criminal or civil proceedings.[127] This is an inherent consequence of the Internet's architecture with its cascade structure: mere conduit (Article 12); caching (Article 13); and hosting (Article 14 of the E-Commerce Directive). As such, even if ISPs would benefit from a differentiated and graduated approach[128] with regard to their liability, and corresponding to the robustness of their services,[129] the effective identification of the individual concerned faces shrinking technological hurdles. AG Szpunar warned that "any general obligation to identify and register users could nevertheless lead to a system of liability applicable to intermediary service providers that would no longer be consistent with [Article 15 of the E-Commerce Directive]",[130] a big leap away from the ISPs' neutrality principle.[131] In the online realm, it matters little at what level of the Internet architecture an interference with the right to anonymity appears. Effectiveness is the creed, and as the principle of proportionality dictates, the procedural rules should be designed in such a way that the court actions concerning ISP's activities could prevent and rapidly terminate any impairments of third parties' interests.[132] Article 8 of Directive 2004/48, in particular, provides for right of information with regard to potential infringement of an IPR, handled via a court order, although no prejudice shall be made to protection of confidentiality of information sources or the processing of personal data. This requires simultaneous compliance with the right to information and the right to protection of personal data.[133] It is now clear that an unlimited refusal to provide information on the basis of data protection of a third party, frustrates the right to information, and as such infringes the right to an effective remedy and the right to intellectual property.[134] Against all this pressure, the right to defend one's self, guaranteed under Article 48 of the Charter must continue to play an important part.[135]

32 The Court's approach may look odd considering that there is no specific EU legislation prescribing

126 See also Rosatti E., Intermediary IP injunctions in the EU and UK experiences: when less (harmonization) is more?, p. 17, available at <https://ssrn.com/abstract=2891042> (accessed on 7 March 2017).

127 Judgment of the Court in Patrick Breyer v Bundesrepublik Deutschland, ECLI:EU:C:2016:779, para 46 and 48.

128 Recommendation CM/Rec(2011)7 of the Committee of Ministers to Member States on a new notion of media (adopted on 21 September 2011) or Opinion of Advocate General Szpunar in Mc Fadden, ECLI:EU:C:2016:170, para 131.

129 Opinion of Advocate General Szpunar in Mc Fadden, ECLI:EU:C:2016:170 and Husovec M., supra note xii.

130 Opinion of Advocate General Szpunar in Mc Fadden, ECLI:EU:C:2016:170, para 143.

131 Opinion of Advocate General Jääskinen in L'Oréal, para 115.

132 Article 18 of the E-Commerce Directive and Judgement of the Court of 12 July 2011, L'Oréal, C-324/09, ECLI:EU:C:2011:474, para 133.

133 Judgment of the Court in Coty Germany GmbH v Stadtsparkasse Magdeburg, ECLI:EU:C:2015:485, para 28.

134 Ibid, paras 37-38.

135 Proposal for a Directive of the European Parliament and of the Council on copyright in the Digital Single Market (COM(2016) 593 final), Article 13(2) also emphasizes the right of redress: "*Member States shall ensure that the service providers referred to in paragraph 1 put in place effective mechanisms, including for complaint and redress, that are available to users in case of disputes over the application of the measures referred to in paragraph 1.*".

mandatory retention of data for the purpose of enforcement of copyright in the online environment. As mentioned earlier, nation-specific information is needed to fill the final gaps; particularly as regards data retention, disclosure, and initiation of court's proceedings. Leading the proportionality analysis of identification measures enforced upon ISPs could then have the character of a mere technical exercise. However, a national judge can also fill other important lacunas left by the Court. The Court's dictum suggests the national judge must assess whether the injunction served upon the ISP would *effectively* work in the desired *dissuasive* manner. It does not finally prescribe the manner in which the judge should lead their analysis, and determine whether the contemplated measure goes or does not go beyond what is strictly necessary. The analysis can be more than technical as a matter of course. This would require the abandonment of the formalistic understanding of the basic proportionality test, and the allowance of important extra-legal considerations[136] arising from social, economic, political, and psychological particularities of each Member State. It is also possible to read this interpretation from the aim at which such an analysis should arrive, which is (soft) behavioural - "dissuasive" by nature. The national judge's role could then be prognostic, normative and diagnostic at the same time,[137] and ready to answer:

- how many local ISPs could be affected by such injunctions involving identification measures sought by third parties protecting their rights, and how many local ISPs could be compelled to discontinue offering communication networks due to mandatory compliance with the local data protection laws;

- what is the general level of trust of citizens towards law enforcement, local ISPs or IT security in a particular sector, and what is the general level of privacy awareness;[138]

- how difficult would it be to enforce the rights of right holders against alleged infringers, and what legal guarantees individuals whose data can be disclose dispose of under national law; or

- what role open Wi-Fi networks play in meaningful local civic participation, and could a fragmentation of political and social discussions occur?

33 These aspects differ dramatically from one Member State to another. Although the analysis of the national court will proceed with strong influence from the CJEU, significant room is left for a fully-fledged nation-specific contextual[139] examination. The Court acknowledged on a previous occasion that putting a complete end to the infringements of rights is an impossible goal to attain; in *re Mc Fadden*, the Court perhaps believed that by switching the default rules, there would be less space to circumvent the law in one way or another and achieve the stated goal.[140] However, targeting by dissuasion and chilling effects are very difficult, perhaps impossible, to reconcile. Dissuasive techniques are designed to constrain people's choices; *mutadis mutandis*, personal autonomy would have difficulties in finding its place in the analysis.

F. Conclusion

34 Arguments have long been heard that chilling effects represent an overstated legal argument,[141] an ephemeral phenomenon,[142] and that the procedural guarantees developed by the CJEU are sufficiently strong to protect both the interest in privacy (autonomy) and the interest in open communication and discussion. However, a stream of cautionary cases arose out of specific political and economic circumstances, for example, during the Cold War period. More recent examples include the *Schrems* case. These moments will come again, in a different form. To preserve the guarantees developed by the procedural scheme of human rights, relying on the habitual insensitivity developed by users as a justification for the reductionist analytical frame, does not seem the correct road to travel in this regard. Nor is the blind search for maximising security and efficiency in the online world.

35 Turning away from the reductionist position, any analysis should acknowledge that at the confluence of the right to private life and freedom of expression, the right to anonymity plays a role in the "cartelization" of the two rights in the online environment. It means that, under certain factual circumstances, concurrent interference

136 See Giovanella I. F., de Rosnay M. D., Community wireless networks, intermediary liability and the McFadden CJEU case, Communications Law, Bloomsbury, Wiley, 2017, 22 (1), p. 17.

137 Foucault M., Discipline and Punish, Vintage Books, 1995, p. 19.

138 Rodrıguez-Priego N., van Bavel R., Monteleone S., The disconnection between privacy notices and information disclosure: an online experiment, Econ Polit (2016) 33, pp. 433–461.

139 Ohm P., supra note lix, pp. 1762 to 1764 and Nissenbaum H., Privacy as Contextual Integrity, 79 WASH. L. REV. 119, 154 (2004).

140 Judgement of the Court in UPC Telekabel Wien, Case C-314/12, ECLI:EU:C:2014:192, para 60.

141 Penney J. W., Chilling Effects: Online Surveillance and Wikipedia Use, 31 Berkeley Tech. L.J. 117 (2016).

142 Ibid.

and remedies could be envisaged with respect to the two rights in question. Hence, strengthening or weakening anonymity in the online world affects the right to private life and freedom of expression and information simultaneously, and in the balancing exercise, these rights reinforce each other. Reductionism does not accommodate human rights in their full breadth. Therefore, one must not only recall that upholding anonymity, legally and technologically, bears the risk of unaccountable free speech, and renders the protection of the rights of third parties ineffective. To the same extent, curbing one's privacy by imposing mandatory real-identity measures, outlawing end-to-end encryption, and proliferating surveillance technologies, can severely deter an individual from the legitimate exercise of his or her right to freedom of expression and information. One must also recall that, with respect to the balancing test, the ECtHR has held that the diversity in practice among Member States as to the weighting of competing interests of respect for private life and freedom of expression calls for a wide margin of discretion, a doctrine embodying the proportionality principle,[143] and the national judge should be rightly called upon to exercise such discretion. This article argued against a purely technical reasoning, bound to lead to dismissive stance concerning extra-legal considerations, and suggested taking chilling effects seriously. Multi-level analysis of the interdependence of human rights against the backdrop of individual Member State particularities may constitute a starting point in any attempt to guide national judges in the latter direction.

143 Judgment of the European Court of Human Rights, Mosley vs UK, paras 108-110.