Written submission from Dr Guido Noto La Diega et al, NINSO Northumbria Internet & Society Research Group (RTP0011)

"The Right to Privacy (Article 8) and the Digital Revolution inquiry"

Written evidence submitted on behalf of NINSO (Northumbria Internet & Society Research Group).[1] (Contributors: Dr Guido Noto La Diega, Claire Bessant, Daria Onitiu and Rachel Allsopp)

1. **Are some uses of data by private companies so intrusive that states would be failing in their duty to protect human rights if they did not intervene? If so, what uses are too intrusive, and what rights are potentially at issue?**

1.1. The relevant rights which are potentially at issue are primarily the right to private life (pursuant to ECHR Article 8 and EU charter Article 7) and the right to data protection (under EU Charter Article 8), as well as the right to privacy (under UDHR Article 12).

1.2. There exists rich case law in particular on ECHR Article 8 in the context of images being disclosed by private companies, such as news organisations, though less so on data being mined by bodies such as Facebook or used for marketing. Thus, it is less clear what, at a European level, is classed as intrusive in those settings.

1.3. What is 'so intrusive' is undoubtedly a difficult question – what one person may consider to be intrusive, another person may not. For example, in the case of *Google v Vidal-Hall,*[2] a case which involved the circumvention of the 'Do Not Track' setting by Google, few people would

[1] NINSO (Northumbria Internet & Society Research Interest Group) is multidisciplinary research unit consisting of researchers from law, business, social sciences, computer science, engineering, and architecture, with a research interest at the intersection of internet and society. For more information please see: https://www.northumbria.ac.uk/about-us/academic-departments/northumbria-law-school/law-research/ninso-the-northumbria-internet-and-society-research-interest-group/

[2] *Google Inc. v Judith Vidal-Hall, Robert Hann, Marc Bradshaw v The Information Commissioner* [2015] EWCA Civ 311

have felt compelled to take that case as far as it went, and yet the claimant managed to receive compensation for the mere distress originating from the knowledge of their data being unauthorisedly accessed by private companies.

1.4. Everyone, including people known to the public, has a legitimate expectation that their private life will be protected.[3] However, this is not necessarily a conclusive factor.[4] The Court's case-law mainly presupposes the individual's right to control the use of their image, including the right to refuse publication thereof. This is demonstrated in the case of *Reklos and Davourlis v. Greece,* in which photographs of a newborn baby were taken in a private clinic without the parents' prior consent and the negatives retained.[5]

1.5. When it comes to the protection of personal data which are in the public domain, the fact that information is already in the public domain will not necessarily remove the protection of Article 8. This was demonstrated in *Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland*.[6] Where there has been compilation of data on a particular individual, processing or use of personal data or publication of the material concerned in a manner or degree beyond that normally foreseeable, private-life considerations arise.[7] In this case, the Court found that the data collected, processed and published by newspapers, providing details of the taxable income and taxable assets of a large number of individuals, clearly concerned their private life, notwithstanding the fact that, under domestic law, the public had the possibility of accessing those data, subject to certain rules.[8] The domestic law must afford appropriate safeguards to prevent any such use of personal data as may be inconsistent with the guarantees of Article 8. Significantly, the

[3] *Von Hannover v. Germany* (no. 2) [GC], §§ 50-53 and 95-99; *Sciacca v. Italy*, § 29; *Reklos and Davourlis v. Greece*, § 40; *Alkaya v. Turkey* (protecting the private address of a famous actress).
[4] *Bărbulescu v. Romania [*GC], §§ 73.
[5] *Reklos and Davourlis v. Greece,* §§ 40 and 43. See also *Von Hannover v Germany* (no. 2) [GC] § 96
[6] *Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland* [GC], § 134
[7] Ibid § 136
[8] Ibid § 138

Court noted that Article 8 provided for the right to a form of informational self-determination, allowing individuals to rely on their right to privacy as regards data which, albeit neutral, are collected, processed and disseminated collectively and in such a form or manner that the Article 8 rights of the individuals concerned are engaged.[9] Accordingly, we recommend that guidelines be issued to clarify that data in the public domain must be processed pursuant to the EU Charter and the ECHR, thus making unenforceable the private actors' attempt to side-step human rights' safeguards by contractual means.[10]

1.6. *M.L. and W.W. v. Germany*[11] dealt for the first time with the press archives on the internet containing news which has previously been reported[12] and the refusal of the applicants' request to oblige media organisations to anonymise on-line archive material concerning their criminal trial and conviction.[13] This situation is to be distinguished from cases in which individuals exercise their data protection rights with respect to their personal information which is published on the internet and which, by means of search engines,[14] may be accessed and retrieved by third parties and used for profiling purposes.[15]

1.7. Search engines such as Google play a key role in ensuring the effectiveness of the rights to privacy and data protection. This was made clear in the seminal *Google Spain*[16] case that introduced the so-called right to be forgotten, which is today provided by the EU General Data Protection Regulation (GDPR) and the Data Protection Act 2018. The

[9] Ibid § 137, see also § 198

[10] For example, Grindr, dating app for men who have sex with men, in their privacy policy expressly claims that the data the users indicate in their profile, including HIV data, is public. See Grindr Privacy and Cookie Policy, effective as of 3 December 2018, <https://www.grindr.com/privacy-policy/> accessed 31 January 2019. On the (mis)use of personal data by dating apps such as Grindr see Guido Noto La Diega, 'Grinding privacy in the Internet of Bodies. An empirical qualitative research on dating mobile applications for men who have sex with men', in Ronald Leenes, Rosamunde van Brakel, Serge Gutwirth and Paul De Hert (eds*), Data Protection and Privacy: The Internet of Bodies* (Hart 2018) 21-70.

[11] *M.L. and W.W. v. Germany*

[12] Ibid § 90 and § 102

[13] Ibid § 116

[14] Ibid § 91

[15] Ibid § 97

[16] C 131/12 *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González* (CJEU).

Court of Justice found in favour of a Spanish citizen whose information on past social security debts from 12 years before was still shown in Google searches. For the purposes of this inquiry it is important to note that the Court pointed that processing of personal data carried out by Google Search was 'liable to affect significantly the fundamental rights to privacy and to the protection of personal data.'[17] Moving on to the intrusiveness, it was stated that 'the effect of the interference with those rights of the data subject is heightened on account of the important role played by the internet and search engines in modern society.'[18] Lawmakers and policy makers, therefore, should be well aware of the importance of ensuring a high protection of personal data and regulating the actions of the most powerful players of the internet: they have an unprecedented role in enforcing fundamental human rights, including privacy, data protection, and private life. Whilst strong data protection laws and policies are crucial, they must be balanced with competing interests (e.g. freedom of expression) and its enforcement be context-dependent.[19]

1.8. Moreover, there is not only the negative obligation not to interfere with the individuals' private life.[20] Member States also have positive obligations to ensure that Article 8 rights are respected even as between private parties. In particular, although the object of Article 8 is essentially that of protecting the individual against arbitrary interference by the public authorities, it does not merely compel the State to abstain from such interference. In addition to this primarily negative undertaking, there may be positive obligations inherent in an effective respect for private life.[21] These obligations may involve the adoption of measures designed to secure respect for private life even in the sphere of the relations of

[17] Ibid [80].

[18] Ibid [80]. See also C-509/09 and C-161/10 *eDate Advertising and Others* [45].

[19] As noted ibid [81], even though the data subject's rights under Articles 7 and 8 of the EU Charter override, as a general rule, that interest of internet users to access information, 'balance may however depend, in specific cases, on the nature of the information in question and its sensitivity for the data subject's private life and on the interest of the public in having that information, an interest which may vary, in particular, according to the role played by the data subject in public life.'

[20] *Kroon and Others v. the Netherlands*, § 31

[21] *Lozovyye v. Russia*, § 36

individuals between themselves. In these instances, it must be asked whether the interference is conducted in accordance with the law. In *Vukota-Bojić v. Switzerland* the Court found a violation of Article 8 due to the lack of clarity and precision in the domestic legal provisions that had served as the legal basis of her surveillance by her insurance company after an accident.[22]

1.9. A prominent example of a ruling against an emanation of a State for private companies' privacy-infringing behaviours is the landmark case *Schrems v Data Protection Commissioner*.[23] An Austrian citizen was concerned by Facebook transferring its users' personal data in the US, where the level of data protection is lower than in Europe and it perceived that there are little safeguards against surveillance. The EU Court of Justice decided to declare invalid the legal instrument that allowed Facebook – and other private entities – to transfer European data to the US (the so-called Safe Harbour Decision). In that case, the Court underlined the 'importance of both the fundamental right to respect for private life, guaranteed by Article 7 of the Charter, and the fundamental right to the protection of personal data, guaranteed by Article 8.'[24]

2. Are consumers and individuals aware of how their data is being used, and do they have sufficient real choice to consent to this?

2.1. No, individuals are not aware of how their data is being used and do not have sufficient choice to consent to such data use. Privacy policies and Terms of Service are too long, difficult to understand, difficult to find, and often unenforceable.[25]

---

[22] *Vukota-Bojić v. Switzerland*; See also *Delfi v Estonia* (though more recent cases go in a partly different direction)

[23] C 362/14 *Maximillian Schrems v Data Protection Commissioner* (CJEU).

[24] Ibid [39]. See also *Rijkeboer*, C-553/07, [47]; *Digital Rights Ireland and Others*, C-293/12 and C-594/12, [53]; and *Google Spain and Google*, C-131/12, [53], [66], and [74].

[25] With regards to the privacy policies and terms of service in smart home contexts see Guido Noto La Diega and Ian Walden, 'Contracting for the 'Internet of Things': Looking into the Nest' (2016) 2 European Journal of Law & Technology 1-38. In the field of mobile applications for men who have sex with men see, Noto La Diega (n 10) 21.

2.2. In regards to the element of 'real choice', following the implementation of the GDPR, increasingly pop-ups are appearing on websites which require individuals to either agree to their data being used, the use of cookies etc or to not access material on that site at all. This is not a choice.

3. What regulation is necessary and proportionate to protect individual rights without interfering unduly with freedom to use and develop new technology?

3.1. There is already a great deal of regulation in place. The difficulty is that corporations/organisations are interpreting the existing laws and new ones such as the GDPR as a tick box exercise, thus not really giving effect to the spirit behind those laws (they are essentially acting in such a way that they do not technically infringe the law but without really allowing individuals autonomy to decide how their information is used).

3.2. The first step should be to collect all existing laws and regulations and assess whether they are consistent. Secondly, one should try and take a holistic, evidence-based approach and amend existing laws only if the fault is in the law itself. This could take the form of a revision of the eCommerce Regulations, of the ePrivacy Regulations or the issuing of guidance on new technologies, such as blockchain.[26] It seems likely that the problem will not be solved by more regulation per se, but by better enforcement, assisted by authoritative guidelines.

3.3. Finally, from our experience, whilst most laws regulate privacy in an adequate manner, an element that should be changed is their binding character. Many regulations can be overridden by private companies by contractual means[27] and this should not be allowed.[28]

---

[26] Following the example of the French Data Protection Authority: CNIL, Blockchain. *Premiers éléments d'analyse de la CNIL* (2018). Cf. Guido Noto La Diega and James Stacey, 'Can Permissionless Blockchains be Regulated and Resolve some of the Problems of Copyright Law?', in Massimo Ragnedda and Giuseppe Destefanis, *Blockchain and Web 3.0: Social, Economic, and Technological Challenges* (Routledge 2019).

[27] See, for example, eCommerce Regulations, reg 20.

[28] Cf. Rossana Ducato and Alain Strowel, 'Limitations to Text and Data Mining and Consumer Empowerment: Making the Case for a Right to Machine Legibility' (forthcoming) IIC.

4. **If action is needed, how much can be done at national level, and how much needs international cooperation?**

4.1. What is undoubtedly required is a serious commitment at an international level (Council of Europe, UN), but with a pragmatic focus on a national level, while ensuring convergence with EU rules.

5. **To what extent do international human rights standards, such as the UN Guiding Principles on Business and Human Rights, have a role to play in preventing private companies from breaching individuals' rights to privacy?**

5.1. The UN Guiding Principles on Business and Human Rights (The UN Guiding Principles) may serve as a common framework and a reference point for the regulation of big data issues including privacy concerns, and the formulation of global standards for the effective use of big data in light of international human rights law, as set out below.

5.2. The operational framework of due diligence enables the introduction of a human rights methodology in the corporations' activities, which have an actual or potential adverse impact on individual liberties. Due diligence in conjunction with the 'knowledge and showing principle'[29] requires that a corporation knows the risks that big data and algorithmic decision-making pose to privacy and is able to show that the collection, storage and processing of data is compliant with human rights. In other words, the UN Guiding Principles apply to the extent that corporations conduct due diligence to understand and remedy the impact of the collection and storage of data, in light of any privacy and human rights concerns.[30]

5.3. Moreover, the UN Guiding Principles and the responsibility of due diligence illustrate an important reference point in introducing a human rights methodology into a company's policy on big data issues, with a

[29] Human Rights Council 'Report of the Special Representative of the Secretary General on the issue of human rights and transnational corporations and other business enterprises, John Ruggie: Business and human rights: further steps toward the operationalization of the "protect, respect and remedy" framework' (9 April 2010) A/HRC/14/27 [80]

[30] David Nersessian, 'the law and ethics of big data analytics: A new role for international human rights in the search for global standards' (2018) 61 (6) Business Horizons 845, 851.

view to the formulation of guidelines on the collection and storage of data. This premise is important regarding the rapid advances of artificial Intelligence including the varying risks data driven strategies pose on human rights. In this respect, a human rights impact assessment entailing the exercise of due diligence with regard to big data issues may accelerate the development of regulatory responses in light of the UN Guiding Principles, providing for a holistic outlook to identify actual and potential harms a corporations' conduct has on the right of privacy. For instance, the BSR, a global non-profit organization recently publish a series of reports on how to implement international human rights due diligence in the context of AI.[31]

5.4. Finally, a corporations' responsibility to conduct due diligence may provide for the basis to strengthen international human rights standards, ensuring that fundamental values are embedded in the use of big data and sophisticated algorithms. Under international law, any interference with the right of privacy requires an examination of the requirement of reasonableness, that any interference must be proportional to the end sought and necessary in the circumstances of the case. The responsibility of due diligence could specify that human rights considerations are embedded in the collection of information, the development of algorithms and the processing of data. This '*privacy by design*' approach in conducting due diligence could strengthen existing international human rights obligations and data protection laws on the regional and national level.

5.5. Nevertheless, because due diligence is an obligation of conduct rather than result, there is the need for a robust international framework that ensures the effective enforcement of international human rights obligations. This premise is based on the argument that the corporation's implementation of the UN Guiding Principles rests on their voluntary

[31] Dunstan Allison-Hope and Mark Hodge, Paper 1: Why a Rights-Based Approach? (BSR Working Paper, August 2018) < https://www.bsr.org/reports/BSR-Artificial-Intelligence-A-Rights-Based-Blueprint-for-Business-Paper-01.pdf> accessed 20 November 2018

initiative.[32] The obligations in the UN Guiding Principles rest on the concept of 'differentiated but complementary responsibilities', whereby states maintain a duty to protect against human rights abuses by third parties building on the corporation's respect for international human rights norms.[33] Indeed, states have the duty to respect international human rights and to establish a judicial mechanism in enforcing those rights.[34] However, the UN Guiding Principles itself are not binding and the corporation's respect for human rights rests on their voluntary initiative.[35] Accordingly, the UN Guiding Principles' terminological separation of a corporations' responsibility and a states' duty to protect international human rights law indicates that (a) the obligation of due diligence needs to be supported by a clear complementary framework that specifies the steps that need to be taken in minimising the risks and privacy concerns posed by big data strategies and algorithmic decision-making; and (b) the need for further initiatives for promotion and the implementation of the Guiding Principles.

5.6. Another problem with the UN Guiding Principles is that it does not possess an effective enforcement mechanism. This argument is based on an interpretation of the principle of complementarity, which builds on the consensual commitment of corporation rather than emphasising notions of accountability. Indeed, the Working Group concerning human rights and transnational corporations and other business enterprises, aims the promotion and the implementation of the Guiding Principles.[36] Within this

[32] Human Rights Council 'Promotion and Protection of All Human Rights, Civil, Political, Economic, Social and Cultural Rights, Including the Right to Development: Protect, Respect and Remedy: a Framework for Business and Human Rights' (7 April 2008) A/HRC/8/5 [107].
[33] Human Rights Council 'Promotion and Protection of All Human Rights, Civil, Political, Economic, Social and Cultural Rights, Including the Right to Development: Protect, Respect and Remedy: a Framework for Business and Human Rights' (7 April 2008) A/HRC/8/5 [9].
[34] Human Rights Council 'Report of the Special Representative of the Secretary General on the issue of human rights and transnational corporations and other business enterprises, John Ruggie: Business and human rights: further steps toward the operationalization of the "protect, respect and remedy" framework' (9 April 2010) A/HRC/14/27 [103].
[35] Human Rights Council 'Promotion and Protection of All Human Rights, Civil, Political, Economic, Social and Cultural Rights, Including the Right to Development: Protect, Respect and Remedy: a Framework for Business and Human Rights' (7 April 2008) A/HRC/8/5 [107]; cf Jens Schierbeck, 'Recasting Corporate Policy for Human Rights Purposes' in Michael K Addo (ed), *Human Rights Standards and the Responsibility of Transnational Corporations* (Kluwer Law International 1999) 85.
[36] Gonzalo Berron, 'Economic Power, Democracy and Human Rights: A New International Debate on Human Rights and Corporations' (2014) 20 Sur- International Journal on Human Rights 123, 126.

context, the Working Group does not possess a 'command and control' mechanism, implying no ability to impose sanctions in case of non-compliance.[37] While the UN Guiding Principles may have a positive impact, introducing human rights considerations into the collection, storing and processing of data, it is important to ensure that due diligence should not merely illustrate mere practice for the management of data but set the parameters for the coherent and effective enforcement of international human rights values in the future.

5.7. However, it is important to note that the framework of the principle complementary illustrates a combination of legal solutions and voluntary initiatives.[38] This framework may prove useful, whereby there is no universal formula yet that minimises the risks and privacy concerns posed by big data. Accordingly, the UN Guiding Principles do illustrate a good starting point for a common framework for an international approach concerning the regulation of the use of big data. Because analysing the impact of big data and advances in AI on individual liberties is an ongoing process, a soft law approach is helpful, to dismantle avenues that ensure effective regulatory responses with regard to big data issues and algorithmic decision-making. In this respect, one recommendation would suggest an emphasis on more voluntary initiatives in cooperation with private entities, in ensuring transparency of algorithmic decisions (i.e. revealing the procedure by which an inference has been reached) and transparency concerning the collection of data from data providers and product innovators.[39]

31 January 2019

---

[37] Michael K Addo, 'The Reality of the United Nations Guiding Principles on Business and Human Rights' (2014) 14 (1) H.R.L.Rev 133, 137; Human Rights Council 'Promotion and Protection of All Human Rights, Civil, Political, Economic, Social and Cultural Rights, Including the Right to Development: Protect, Respect and Remedy: a Framework for Business and Human Rights' (7 April 2008) A/HRC/8/5 [107].
[38] Peter T Muchlinski, *Multinational Enterprises & The Law* (OUP 2007) 525.
[39] 'Submission by the Human Rights, Big Data and Technology Project ('HRBDT' and the Essex Business and Human Rights Project ('EBHR') to the UN Working Group on Business and Human Rights ('UNWG') for the consultation process to inform its 2019 Report to the UN General Assembly' (30 May 2018) < https://www.ohchr.org/Documents/Issues/Business/WGSubmissions/2018/Essex.pdf> accessed 28 January 2019 [22].