CHECK AGAINST DELIVERY

Thomas More Lecture 2018 – Lincoln's Inn, 29 November 2018

'Big Data': The ECtHR as facilitator or guardian?[1]

Tim Eicke, Judge, European Court of Human Rights

I. Introduction

1. In his seminal work, Sir Thomas More's protagonist Hytholday posits a 'utopia' in which society is fair and equal, in the utilitarian sense. Utopia was underpinned by a programme of extensive, mass surveillance – of convicts by their wardens, slaves their masters, and even citizens by their elected officials. More's surveillance State provided inspiration (in part) for Orwell's 1984. The risks and dangers of State surveillance of this kind have been rich materials for authors and artists, and a source of concern and then action by civil society, including through the Courts. That work continues, and the Strasbourg Court (as many of you will know) decided the case of *Big Brother Watch*[2] earlier this term. However, today, this is not the aspect of More's surveillance State I wish to focus on.
2. My concern is with the other, more subtle but potentially more invasive, form of surveillance he identifies – that of citizens between themselves. More defines, in 'Utopia', a world in which there is no private space. Garden doors are '*never locked nor bolted; so easy to be opened, that they will follow the least drawing of a finger, and shut again alone. Whoso will, may go in, for there is nothing within the houses that is private, or any man's own*'[3]. Family members monitor and sanction one another so '*nothing can be so secretly spoken or done at the table*'[4]. Citizens '*have little… to loiter…no cloak or pretence to idleness*', '*no lurking corners… places of wicked counsels or unlawful assemblies*'[5], each person being permanently '*under the eyes of every man*'.
3. More could not have anticipated the resonance of that description to many who use the internet, which acts and functions in many respects as a global village, with all that entails. The notion of ready access to data and information means each of us is only a

---

[1] I am very grateful to Anita Rao, stagiaire at the Court, Pegasus Scholar and barrister at Field Court Chambers for all her hard work and detailed research as well as our stimulating discussions in the course of preparing this talk

[2] *Big Brother Watch and Others v. the United Kingdom* (nos. 58170/13 and 2 others, 13 September 2018)

[3] Chapter II, Utopia: Containing an Impartial History of the Manners, Customs, Polity, Government, &c. of that Island, translated and with commentary from the Rev T.F. Dibden (J. Newbery) 1808 (Link available at: https://books.google.fr/books/about/Utopia.html?id=HnIJAAAAQAAJ&printsec=frontcover&source=kp_read_button&redir_esc=y#v=onepage&q&f=false) (last accessed on 22 November 2018)

[4] Chapter V, Utopia (ibid)

[5] Chapter VI, Utopia (ibid)

Google search away from being able to know private and intimate details about one another, that is if we do not already know them through Instagram, Twitter or Facebook. Social media newsfeeds and posts allow them and us to surveil other citizens. Using these sites, we participate in this global village, inviting approval and disapproval by like, retweet or post and, on many occasions, participating in the system of rewards and sanctions that ensure compliance with our values or norms. By equal token, As Professor Nemitz, Principal Adviser in the European Commission and visiting Professor at the College of Europe in Bruges, suggested in a recent paper, '*collecting [our] personal data for profit and profiling… based on our behavior online and offline'*, those intermediaries through whom we use the internet *'know more about us than our family or friends'*[6]. We have all heard the apocryphal story in which algorithms used by Target, the US discount store, for targeted advertising in 2012 identified a teenage girl as pregnant before she had told her father. The global village comes with its disadvantages, as well as advantages.

4. The acquisition, use and disposal of data by private internet intermediaries poses challenges to how we conceive of our human rights, how we protect them, and if indeed, we should do so. There has been increasing recognition of the dangers of what has been described as '*surveillance capitalism'*[7] – the market built around the acquisition and use of personal data for profit. Perhaps for this reason, there has been a proliferation of action in this sphere over the last decade. A certain amount of progress has undoubtedly been made in defining ethical standards for the industry by bodies such as the Institute of Electrical and Electronics Engineers (IEEE) Standards Association, the Internet Engineering Task Force (IETF), the Internet Architecture Board (IAB), and the Internet Society. There is a real question whether self-regulation, such as the voluntary adoption of ethical standards, alone will be sufficient. As more of the world is online, and begins to conduct their life virtually, the application of enforceable legal rules is likely to be required. This is also reflected in the work being undertaken by the Council of Europe and UN, the latter concluding its second World Data Forum last month.

II. The problem

5. We are, at present, in a period of significant change – as we saw in the news this year alone: Facebook was reportedly fined record amounts for breaching people's data

[6] P Nemitz 2018, Constitutional democracy and technology in the age of artificial intelligence Phil. Trans. R. Soc. A 376
[7] S Zuboff 2015, Big Other: Surveillance Capitalism and the Prospects of an Information Civilization, Journal of Information Technology (2015) 30, 75–89

protection in association with Cambridge Analytica[8], while Google reportedly failed to disclose a similar data breach[9], Away from the big five[10] - who go by the catchy acronym of FAMGA - an American insurer has reportedly now made any offer conditional on their insured using FitBits and gym memberships[11] - human versions of the black box car insurance. Looking beyond these – purportedly commercial aspects of the story – real concerns have been expressed that the democratic process is being subverted by the use of our personal data to tailor our experience of the internet (creating 'thought bubbles', and generating updates and search results which we may wish to see – a bespoke internet experience for each person which limits our access to information and debate)., Conversely, the omission of online information about third parties (exercising their so called right to be forgotten) is capable of creating a partial picture of them, with few (if any) of us knowing why or how[12].

6. As technology progresses, society has been required to respond. The UN World Data Forums, GDPR, the modernisation of the Council of Europe's Data Convention (Convention 108, which the UK was one of the first to sign) and the daily news stories about Apple, Facebook and Google proposing voluntary self-regulation evidence the level of concern. Only two weeks ago, the Council of Europe published three draft 'soft law' instruments, addressing the human rights implications, and manipulative potential, of automatic algorithmic processes, and considering the risks posed by artificial intelligence to our human rights[13]. The Council of Europe's Steering Committee on Media and the Information Society is sitting to discuss these documents as we speak. Evolving concerns about big data have prompted new responses.
7. That having been said, the story is far from being one sided. As Professor Alemanno noted in a recent article, big data is equally capable of serving the public good[14] whether by helping emergency services coordinate their responses to crises, or finding out where the most vulnerable people are in the aftermath of an attack, where the epicentre is or how

[8] https://www.theguardian.com/technology/2018/oct/25/facebook-fined-uk-privacy-access-user-data-cambridge-analytica
[9] A bug in Google+ enabled third-party app developers to access the data of users who granted permission and also that of their friends (who had not)
[10] Apple, Microsoft, Google, Facebook and Amazon
[11] See, for example, https://www.reuters.com/article/us-manulife-financi-john-hancock-lifeins/strap-on-the-fitbit-john-hancock-to-sell-only-interactive-life-insurance-idUSKCN1LZ1WL
[12] While this is only in response to searches against their name, it is difficult to identify how else (speaking practically) one would be able to access the relevant information. In relation to the global scope of any ban, this is presently before the CJEU in *Google France* (C-157/17).
[13] Published at https://www.coe.int/en/web/freedom-expression/msi-aut#{%2232639232%22:[]}
[14] This was a theme explored, in particular, by the UN World Forum last month in several of its plenary sessions.

a pandemic (like Zika) is spreading[15]. Facebook allows individuals to mark themselves as 'safe' in many cases, and the European Parliament voted only two weeks ago for a "reverse 112" system by which citizens close to a major emergency or disaster would be sent a text or app alerts . Big data may be capable of making the difference in disaster zone management, where real time data is available, situations change quickly and life or death decisions are taken under time pressure on incomplete information[16]. Longer term, it may be capable of enabling a better allocation of resources (for example, in urban planning and health, by identifying commonalities in sufferers and signs before the illness deteriorates) and in monitoring how effective a given intervention is[17]..

8. Nevertheless, the human rights implications of big data (for better or worse) are potentially vast. Its cross-jurisdictional reach may require coordination, and action, at an international level.
9. The ability of the Convention to respond to the novelties and evolution of civil society is, of course, not new. Though often said, the Convention must be interpreted in harmony with other relevant international law and soft law, having regard to the existence or absence of international (and European) consensus. As so evocatively put by Judge Rosakis, the Strasbourg judiciary '*do not operate in the splendid isolation of an ivory tower built with material originating solely from the ECHR's interpretative inventions or those of the States party to the Convention*'[18].
10. This point has two aspects. First, it reflects the Convention's nature as a living instrument, which evolves to meet modern challenges – a principle first articulated in *Tyrer*[19] in 1978, a case concerning the of 'birching' of a first time juvenile offender in the Isle of Man. Secondly, it reflects the principles of subsidiarity and the margin of appreciation. Where the challenges are as nuanced and complex as those posed by big data, it is ultimately and properly down to States to decide how to legislate and institute measures in response, and to find the way of dealing with these competing pressures that is right for them, both in line with Convention standards and against the background of the international legal and commercial efforts ongoing in this arena; as long as that is done having regard to (and being seen to have regard to) Convention standards.

[15] A Alemanno, 'Data for Good: Unlocking privately held data for the benefit of the many' (9 European Journal of Risk Regulation 2, 2018)
[16] Alemanno, 2018 (ibid)
[17] Alemanno, 2018 (ibid)
[18] Rozakis, The European Judge as a Comparativist, in Tulane Law Review, 2005, p. 278.
[19] *Tyrer v. the United Kingdom*, 25 April 1978, §31, Series A no. 26

11. With this in mind, I hope this evening to set out the role the Convention and Court may play in this debate – where the Court's case law now is, in terms of setting some of the parameters of debate, and the role it may play going forward in supporting member States in their efforts to grapple with these issues.

III. Where now & where to – 'big data' & the Convention

12. The Court has already repeatedly had cause to recognise the internet's '*accessibility and its capacity to store and communicate vast amounts of information*', which allows it to play '*an important role in enhancing the public's access to news and facilitating the dissemination of information in general"*[20]. This characteristic has been found to be a relevant consideration as to whether restrictions on the printed media[21] or access to broadcast media[22] can be justified. This was on the basis that the internet made for a sufficient substitute.
13. In considering whether the protections afforded by Article 10 are applicable, the Court has, to date, generally demonstrated what has been described as a *'technology blind approach*'[23]. The Court has found its protection to be applicable, in principle, to content disseminated online[24], not least through blogging and the use of social media[25], the hosting of content on a website[26], and the use (in certain circumstances) of Youtube[27]. In a case heard by the Grand Chamber last week, the applicants argued such protections should also extend to a mobile app made available to voters by an opposition party, that allowed them to post and share photographs of invalid ballot papers during Hungary's 2016 referendum on the EU's migrant relocation plans[28].
14. Article 10 protection is of course capable of extending to a wide variety of forms of expression, including photos[29], moving images, and sounds[30]. It has been suggested that it

[20] *Times Newspapers v UK (nos 1 and 2)* (10 March 2009); see also *Delfi AS v Estonia* (no. 64569/09, 16 June 2015) (***Delfi AS***) [133]
[21] *Mouvement Raëlien Suisse v Switzerland* (no. 6354/06, 13 January 2011). It was material to the Court's conclusion that the applicant could continue to disseminate ideas via their website.
[22] *Animal Rights Defenders v UK* (no. 48876/08) ECHR 2013 (***Animal Defenders***). The Court found a restriction on TV and radio justified, relying in part on access to the internet.
[23] L Woods, 'Social media: it is not just about Article 10' extracted in The Law of Social Media (2017)
[24] See *Feret v Belgium* (no 15615/07, 16 July 2009) (***Feret***)*; Neij and Sunde (Pirate Bay) v Sweden* (40397/12, 19 February 2013[24]) (***Pirate Bay***)).
[25] (*Ahmet Yildirim v Turkey* (no. 3111/10, ECHR 12) (***Yildirim***)
[26] *Pirate Bay*
[27] *Cengiz v Turkey* (48226/10 and 14027/11, 1 December 2015) (***Cengiz***)
[28] *Magyar Kétfarkú Kutya Párt v. Hungary* (no. 201/17, 21 November 2018)
[29] *Ashby Donald v France* no 36769/08, 10 January 2013 (***Ashby Donald***), in which the publication of photos on an internet site devoted to fashion which offered fashion photos some for free and some for sale fell within Article 10 as freedom of expression.

may eventually apply to 'likes' and emojis[31] where used to express opinions. As the Court has already extended Article 10 protections to commercial content[32], there is no reason to suppose that, for example, paid likes could not be capable of falling within its scope (even taking into account any sponsorship or employment context). Article 10 is therefore capable of protecting posts from the Kardashians as well as it does those of traditional NGOs and activists.

15. By the same token, just as not all speech is protected, it is likely that not all likes and emojis will merit protection. It has, perhaps rightly, been suggested that the Court would be unlikely to offer a high level of protection to social network speech about what the author was eating or wearing[33]. Such speech is likely to be deemed of little informational value[34] by reference to the public interest (rather than what the public may find interesting). However, while much of what society may search for, tweet about and post may ultimately therefore not readily call for a high level of protection under Article 10, or possibly even fall outside its scope, it nevertheless is likely to be within the "ambit" of that provision so as to engage the protection against discrimination under Article 14.
16. That being said, the Court has implicitly acknowledged in *Big Brother Watch*[35] that, quite apart from their content, posts and likes of this kind may have a different – perhaps increased – importance and informational value in that the associated communications data/meta data is capable of being used to build up a 'profile' of someone in a manner enabling enhanced targeting (of advertising or news) or filtration of content seen. In this context, Article 10 may well be engaged in a different way. Such distorting influences bring into question to what extent the Convention protects a right to autonomous freedom of expression, or indeed meaningful freedom of thought within Article 11. Is there a right to fair and impartial knowledge arising out of the Convention?
17. Some may suggest that the first step in such an argument has already been taken, following the recent Grand Chamber decision *Magyar Helsinki Bizottság*[36]. In that case, the Court (controversially in the eyes of some) recognised a (limited) right of access to information in circumstances where access to that information was instrumental for an individual's exercise of his/her Article 10 rights. Factually, the NGO applicant sought

[30] A*shby Donald; Feret*
[31] Woods, 2017
[32] *Ashby Donald*
[33] Woods, 2017
[34] *Von Hannover v Germany* (40 EHRR 1), *Standard Verlags GmbH v Austria (No 2)* (no 21277/05, 4 June 2009)
[35] Albeit in the context of Article 8
[36]. *Magyar Helsinki Bizottság v. Hungary* (no. 18030/11, 8 November 2016)

information relating to the ex officio work of a defence counsel in order to complete a study on the public defender's system, which the State held but refused access to. Finding a violation of Article 10, the Court observed that the State's failure to provide the information impaired the NGO's right to receive and impart information, which (the Court found) '*struck at the very heart of Article 10'*.

18. Taking that principle further, and '*moving towards the recognition of a right to public interest information*'[37], the Court may yet have to consider to what extent FAMGA and others (in their capacities as holders of public interest information) may be subject to the same responsibilities, and the extent of State obligations to secure it.
19. Beyond the targeting and filtration of information made available through search engines, the right to be forgotten is also capable of having a significant impact on this right, in so far as it *removes* public interest information from the public domain. Currently, under the terms of *Google Spain*, information removed can still be accessed outside the European Union, including in 19 of the Member States of the Council of Europpe. This is, however, under challenge at present[38]. If the right to be forgotten extends worldwide, its potential impact on Article 10 – in the sense of the complete inability to know what has been 'forgotten' - may well increase.
20. In another strand to the argument, the Court has also affirmed that Article 10 imposes on States an obligation not to interfere with the right to receive and impart information[39], including though the internet. The clearest examples of this the cases of *Yildirim, Adkeniz*[40] and *Cengiz.*,In *Yildirim*, the Court found a breach of Article 10 in the context of an incidental shutting down of Google and third-party websites (including the applicant's) as a result of an interim order targeting a website that was the subject of domestic criminal proceedings. By contrast, in *Adkeniz*, which concerned an application by a customer seeking access to a music streaming site, blocked for copyright infringement, the Court found the applicant customer was not a victim. Finally, in *Cengiz*, the Court considered that the blocking of all access to YouTube in Turkey between dates in 2008 and 2010 amounted to a breach of Article 10. It was particularly relevant to the Court that Youtube was a single platform enabling information of specific interest,

[37] The concept was first proposed in TÁRSASÁG A SZABADSÁGJOGOKÉRT v. Hungary (no 37374/05, 14 April 2009)
[38] *Google France* (C-157/17). The opinion of the Advocate General is awaited.
[39] *Loiseau v France* (no 46809/99, 18 November 2003)
[40] *Adkeniz v Turkey* (no. 20877/10, 10 March 2014)

particularly on political and social issues, to be broadcast,, and allowed academic and non-professional journalism to take place.

21. It remains to be seen to what extent, if at all, the principles established by these cases will be developed, qualified or reaffirmed in the pending case of *Kharitonovi.*[41] That case concerns the incidental blocking of the applicant's website by reason of a decision to block a third party website in a way that also blocked the applicant's website (both sites sharing parts of the IP address).
22. That said, it is worth noting that, in both *Yildirim* and *Cengiz*, the status of the respective website (whether Google or Youtube) as a dominant forum for access to information and for expression was treated as critical. This implicit recognition of particular fora on the internet as integral to the exercise of Article 10 rights may well foreshadow formal recognition of the role of the internet *itself* as integral to it. From there, the question arises of whether is it going too far to suggest that there may exist a positive entitlement to access to the internet?
23. To date, the Court has stopped well short of recognising such a right. The furthest the case law has gone is imposing a particular obligation on States, where national law provides for an entitlement to the internet, to make good on that obligation; a point amply made in two prisoner access cases, *Kalda*[42] and *Jankovskis*[43]. In the latter, the Court went as far as holding that where access to the internet was provided for the purposes of education generally, justification for denying a prisoner access to the internet was required (even though national law expressly prevented prisoners having access to the internet). This suggests that any principle of access cannot simply be confined to certain persons, and a more purposive approach may be required.
24. Second, the three Turkish cases may provide some indication of whether, and if so how, account may be taken of the monopoly status (and growing power) of some of the intermediaries moderating our access to the internet. In each of these cases, the importance of the existence of other (effective) venues for freedom of expression was an important factor in the Court's decision. Now, in the context of a monopoly in broadcast media intervention of the State by means of '*positive measures of protection, through its law or practice*' has already been found to be required to support a '*pluralism of views*'

[41] *Kharitonov v Russia* (no. 10795/14).; see also *Kablis v Russia* (no. 59663/17), a case in part concerning the blocking of the applicant's VKontakte account, which may also have a bearing on these principles.
[42] *Kalda v Estonia* (no. 17429/10, 19 January 2016). The Court found that States are not obliged to grant prisoner's access to the internet, but having done so they had to give reasons for preventing access to particular websites.
[43] *Jankovskis v Lithuania* (17 January 2017)

(see *Manole*[44]) the Court noting that '*the State must be the ultimate guarantor of pluralism*' (§99).

25. Targeted or filtered information on the internet may of course also be capable of compromising pluralism. Accordingly, where the policies or practice of a dominant company prevent such '*plurality of views*' (which, ultimately, it is for States to guarantee), this may raise very real issues under Article 10.

26. There may also be a need to take the point wider. Given the relative lack of transparency as to how each company functions, how it undertakes information 'prioritisation', targeting or filtration, or indeed as to how it uses algorithms to process our data, it is, for most, difficult to understand to what extent and in what respects the actions of these companies are affecting our human rights. An obvious recent example is the use of algorithms to deal with inappropriate, illegal and unlawful content. Under the Convention, as many of you will know, hate speech is not protected[45]. However, the right to say things or express opinions that offend, shock, or disturb is[46]. Finding the line between the two, the Court has taken into account nuance and context, proving itself capable of dealing with hateful speech said to be 'just a joke'[47], or ironic[48]. This approach reflects how you or I would approach the same content. This understanding or application of nuance, however, is (at least so far) incapable of being replicated by automation[49]. We all recall Facebook's 2016 removal of the iconic photograph of the naked 9-year old girl fleeing napalm bombs during the Vietnam War as a violation of nudity rules[50] and its earlier removal of pictures of women breastfeeding on similar grounds[51]. We also hear about unacceptable content from terrorist organisations being kept online. There is a separate, and important debate, to be had there as to whether 'bots' should undertake such roles at all. However, the point I wish to make is that, as imperfect as automation presently is, it is (in effect) a black box, the contents of which may well differ from company to company.

---

[44] e.g. see *Manole v Moldova* (no 13936/02) [2009] ECHR 1292

[45] See, for example, Article 17 of the Convention which excludes from protection speech incompatible with the values proclaimed and guaranteed by the Convention

[46] *Handyside v UK* [1976] 1 EHRR 737. This approach also accords with the approach of the UN Special Rapporteur on Freedom of Expression taken on 16 May 2011 [**A/HRC/17/27**] 16 May 2011, and Article 19 of the ICCPR.

[47] *M'Bala v France* (no 25239/13, 20 October 2015)

[48] *Nix v Germany* (no 5285/16, 13 March 2018)

[49] Yeung 2018, A study of the implications of advanced digital technologies (including AI systems) for the concept of responsibility within a human rights framework MSI-AUT(2018)

[50] https://www.theguardian.com/technology/2016/sep/09/facebook-reinstates-napalm-girl-photo

[51] https://www.huffingtonpost.co.uk/2015/03/16/breastfeeding-facebook-nudity-policy_n_6877208.html

27. On another note, if our ability to access some sites may be critical to our Article 10 rights, as the Turkish cases suggest, how does the practice of excluding or blocking certain persons from social media sites fit with the Convention? And does there need to be a judicial remedy?
28. It will already be evident that Article 10 is not the only right capable of being affected by the dominance these companies exert.
29. In many respects, Article 8 has a far more ready application to the problems big data presents. It is, already, the more natural home for claims relating to personal data, not least because such data is well recognised as falling within the scope of personal life and correspondence under Article 8.
30. Principles of data protection of personal data are perhaps the longest standing aspect of Article 8 case law with relevance to this subject. In addition to the GDPR, and its predecessor (Directive 95/46), Convention 108[52] (the Council of Europe's Data Protection Convention) has served to set European standards for data protection which have permeated many of the Court's decisions[53]. Technological change has necessitated development. By the adopting of its 2001 Protocol[54] to, and the recent modernisation of, Convention 108, significant steps have been taken to empower individuals to control access to their data, minimise data held by internet intermediaries and promote understanding of the human rights implications of the processing of our data.
31. While significant and welcome, even the modernised Convention 108 is unable to address the full scope of potential issues arising under Article 8, many of which go well beyond personal data alone. One real difficulty is in explaining why many, if not most, people do not seem to do much to protect their privacy against lawful or unlawful interception. Is it because we no longer care about privacy? Somehow I do not think so. In 1990 Scott McNealy of Sun Microsystems declared privacy dead – '*You already have zero privacy. Get over it*'. Facebook founder, Mark Zuckerberg, said the same in 2010 declaring privacy would no longer be a social norm. But many of us in (and out of) this room would rail against the prospect of living in More's Utopia. As Lord Neuberger expressed extra-

[52] *The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*
[53] See, for example, unlawful data retention by States in *Rotaru v Romania* (no 28341/95, 4 May 2000); and *Amman v Switzerland* (no 27798/95) ECHR 2000-II.
[54] Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows (ETS No. 181)

judicially, people may still care about their privacy even if they do little to protect it[55]. Perhaps instead, it is that, where big data is concerned, the public's sense of risk, well developed in traditional environments, has had little opportunity to develop[56]. Perhaps privacy needs to be rethought to take account of these new risks.

32. Traditionally, of course privacy was thought of by many as akin to secrecy or confidentiality[57]; the door you could lock. Now as we exist in a world where much is placed in the public sphere, can it necessarily be the case that a tendency to post about ones daily life, and divulge details about oneself on social media is evidence of a cultural shift to the effect that all things should be public? Such an approach would not accord with the Court's case law to date – if a celebrity does not give up all privacy simply by being one[58], and ordinary people do not give up all privacy by being outdoors[59] nor when conducting personal business at work[60], then there may be something else going on.
33. Perhaps it is possible to conceive of privacy as determining/controlling the accessibility to ones information[61] - in effect, the right to say when, how and to whom the private details of our lives are disseminated. Another way of putting it is to treat use of our data as subject to a "right to informational self-determination", a concept originally developed as long ago as 1983 by the German Constitutional Court as an expression of the right to human dignity. This would accord with the interpretation of privacy given by the Court in *Benedik*[62] – the leading case on the scope of reasonable expectations of privacy in the digital age – and was built upon in our judgment in *Satakunnan* [63] in which the Grand Chamber found that Article 8 provides for that right, 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 their Article 8 rights may be*

[55] Lord Neuberger 'Is nothing secret? Confidentiality, privacy, freedom of information and whistleblowing in the Internet Age' (2 September 2015)
[56] Lord Neuberger, 2015
[57] So is the view of D Solove in 'Speech, privacy and reputation on the Internet', extracted in The Offensive Internet: Speech, Privacy and Reputation (2010).
[58] *Campbell v UK (*no 13590/88, 25 March 1992); *Von Hannover v Germany* (no 59320/00, 24 June 2004)
[59] *Peck v UK* (no 44647/98, 28 January 2003)
[60] *Bărbulescu v. Romania* (no. 61496/08, 5 September 2017)
[61] Solove, 2010
[62] *Benedik v Slovenia* (62357/14, 24 April 2018). This concerned the legal obligation of an internet access provider to divulge to the police the person details attached to an IP address without the consent of the subscribed, in the event of an investigation into pornography
[63] *Santamedia Oy and Satakunnan v Finland* (no. 931/13, 27 June 2017)

engaged.'[64] The emphasis is on control over how one's data is used and disseminated, rather than whether it is used at all.

34. This conception of privacy would also explain the Court's decision in *Verlags News*[65], in which photos were taken of the applicant at home (with his agreement), but were shared more widely without his consent. A violation of Article 8 was found. It would similarly explain the Court's finding in *Aleksey Ovchinnikov*[66] that there may exist restrictions on the re-reporting of information already in the public domain in a different respect. Away from the case law, it also may explain instinctively why we might be willing to share details of our lives on Facebook with a select group of friends and privacy protections on, but would understandably object if that information was accessed, sought or required more widely.
35. While therefore our conceptions of privacy may have begun to change, what is less clear is how this may affect the scope of the 'reasonable expectation' we may have to privacy. How, for example, might our reasonable expectations of privacy change according to the sorts of information companies can now collect in relation to us? I think here of the logging of how long we spend on sites, how long our mouse hovers over a link, the systematic tracking of our spending[67] and how we got to the site in question. One need only look at Google Analytics to see the extent of the picture one can build from simply what one does on the internet. Metadata is already capable of engaging Article 8[68], but the question of the scope of 'personal information' may yet become more complex. Since the iPhone X, new Apple iPhones unlock in response to facial recognition (whereas its predecessors used only fingerprint access). It seems a short step from there to technology capable of detecting smiling, laughing, crying, or any emotions we display on our faces or even body form. If that is processed to allow technology to better interact with us (care robots are an obvious application[69]), does that not constitutes personal data as well?
36. Is it arguable that there is a certain core of private information which no one should be able to collect? If so, what is it? If we do not go that far, do we nonetheless protect a core

[64] This is also the approach taken in Recommendation CM/Rec(2017)8 on Big-Data for culture, literacy and democracy which states inter alia that everyone can choose to be inscrutable in the digital age and therefore has a right to not have predictions made by algorithms about their cultural attributes, preferences and behaviours.
[65] *Verlags News GmbH and Bobi v Austria* (no 59631/09, 4 Dec 2012).
[66] *Aleksey Ovchinnikov v Russia* (no. 24061/04, 16 December 2010)
[67] Yeung 2018; It is of note the phenomena of changing prices depending on how many times an item is looked at is being investigated by the government, see https://www.gov.uk/government/news/government-and-cma-to-research-targeting-of-consumers-through-personalised-pricing
[68] See *Malone v the United Kingdom* (no 8691/79); and *Benedik*
[69] See, for further detail, Rathenau Institute, van Est and Gerritsen 'Human rights in the robot age' (2017)

of sensitive personal information? Though Article 8 protects personal information which individuals can legitimately expect not to be published without their consent[70], the Court has drawn no bright line preventing the disclosure of a particular category of personal information. However, sensitive data (revealing racial origin, political opinions or religious or other beliefs, or data concerning health, sexual life or relating to criminal convictions) warrants special protection under Convention 108[71] and EU law as well as under the Convention. In *S and Marper*[72], for example, the Court held that the extent of interference with the applicants' right to private life may differ for each of the three categories of personal data retained, retention of cellular samples being particularly intrusive. What this may suggest is that an enhanced consent may be required where sensitive data is concerned.

37. There is also the question to what extent our past attitudes in relation to the information disclosed should have a bearing on our claims to keep it private today? If we seek to keep private that which we willingly disclosed before, for profit or publicity (for example), that may well have a bearing on the outcome, as the Court found in *ML and WW*[73]; a case concerning an application for anonymisation of historic information relating to the applicants' criminal convictions, parts of which the applicants had willingly previous disclosed. However, caution may need to be taken when considering the question of waiver more broadly, as the Court did, in a different context, in *Campbell*[74]. Instinct would also suggest a cautious approach should apply to children and teenagers, not least to afford them a space to learn and develop and in keeping with the need to afford them special protections[75].
38. Further, if we seek to rely on a reasonable expectation of privacy, must we have taken all (all reasonable) steps to protect it? What about those who are technologically less capable? What amounts to all reasonable steps – is it website or app dependent? How can account be taken of technological change? If we fail to use one of those methods (e.g. by forgetting to change our default settings), are we to be taken as having abrogated our right

[70] *Finkilla v Finland* (no. 25576/04, 4 April 2010; *Saaristo v Finland* (no. 184/06, 12 October 2010)
[71] Recommendation CM/Rec(2012)3 (in relation to search engines)
[72] *S and Marper v UK* (App No 30562/04) [2008] ECHR 1581[72] [120]
[73] *ML and WW v Germany* (no 60798/10, 28 June 2018)
[74] *Campbell v the United Kingdom* (no 13590/88, 25 March 1992)
[75] As set out in *K.U. v. Finland* (no. 2872/02, 2 December 2008), on which see below.

to privacy? At present, *Benedik v Slovenia*[76] suggests 'not quite': the Court held that '*not hiding a dynamic IP address, assuming it is possible to do so, cannot be decisive in assessing whether there is a reasonable expectation of privacy in relation to a person's identity*'. However, equally, the online activity of the applicant was factually found to carry a high degree of anonymity.

39. What, therefore, appears to be relevant to any reasonable expectation is the relative anonymity of the activity being undertaken. The Court's case law has so far relied on the right to be anonymous online as one of the defining features of the internet[77]. In the wider context, it is obvious to see why by looking to Article 10[78] - the identification of a government critic, whistle-blower or anonymous blogger would, in many cases, prevent them from acting. But the right to anonymity cannot be absolute[79]. After all, in the context of big data, anonymity may create its own challenges to the protection of human rights. One example arises when considering the collective action problems big data presents, namely where an individual's data is not *in itself* of use but forms part of a wider data set that treats the individual as a member of a group according to gender, age or home area (for example)
40. Using data in this collective sense, companies can draw patterns which they may use to artificially influence a person's emotions or mood or to train or build artificial intelligence. To the extent that companies are using technology and our personal data to build a sufficiently comprehensive picture of all of us to enable them to tell each of us what to do i.e. run more, do more steps and stairs, there may well be a material risk to our autonomy. As both Convention 108, and Article 8 have historically treated personal data as belonging to the individual, this approach may seem to leave little room to address these collective data problems.
41. That said, it is well established that Article 8 also extends to a concept of human dignity – is it arguable that treating people, collectively as data objects, rather than rights holders, undermines their dignity (collectively and individually)[80]?

[76] (62357/14, 24 April 2018) Which concerned the legal obligation of an internet access provider to divulge to the police the person details attached to an IP address without the consent of the subscribed, in the event of an investigation into pornography.
[77] *Delfi AS*
[78].It is notable that The Council of Europe's Committee of Ministers affirmed the principle of anonymity in its Declaration on Freedom of Communication on the Internet (principle 7). The Committee stressed that in order to ensure protection against online surveillance and to enhance the free expression of information and ideas, member States should respect the will of users of the Internet not to disclose their identity.
[79] As recognised in *K.U.*
[80] Yeung, 2018

42. It is similarly well established that Article 8 is capable of extending to what has been called a right to self develop. There are few who would dispute that there is harm done by failing to afford people a space in which to grow, develop, make mistakes and learn from them. This raises particular issues in the context of social media. It is easy to see the risks of a chilling effect in a society where individuals are inhibited from expressing themselves in a private sphere, for fear of the information made public.
43. There are two possible ways the right to self-development may be relevant: First, there is an obvious corollary between the right to self-development and the desire to have past irrelevant misdeeds forgotten; we return to the 'right to be forgotten'. Just as information may be posted on the internet, there may be an equal entitlement to have it removed. Two decisions are worth mentioning in this context. In *MM*[81], the Court observed, in the context of a minor conviction or caution, that as it receded into the past it became a part of the applicant's private life which had to be respected. On the other hand, in *Węgrzynowski*[82], the Court observed that "*It is not the role of judicial authorities to engage in rewriting history by ordering the removal from the public domain of all traces of publications… found to amount to unjustified attacks on individual reputations… the legitimate interest of the public in access to the public Internet archives of the press is protected under Article 10*." This highlights the tension between Articles 8 and 10 in this particular context.
44. Second, a right to true self-development is, in many respects, contingent on access to information and knowledge. Drawing on my earlier observation, to the extent the internet becomes our principal (or only) source of information, if it shows us 'fake news' or only that which confirms what we already believe, or where it cannot guarantee that two users of the same search engine entering the same search terms are seeing the same thing, it fails to act as a neutral or objective source of knowledge to support us in our self-development[83]. There is therefore a question of whether the private companies which tailor our experience of the internet should be able to do so unsupervised or unchecked. In a time where seeing no longer strictly justifies believing, I would pose the following questions: should the internet be neutral? Should there be any obligations of fair content or coverage? How would such obligations work in relation to, say, Twitter (which is designed to provide partial information), or Instagram (which imparts little to no news per

[81] *MM v the United Kingdom* (no 24029/07, 14 November 2012)
[82] *Węgrzynowski and Smolczewski v. Poland* (no. 33846/07, 16 July 2013) (***Węgrzynowski and Smolczewski)***
[83] In addition to potentially interfering with our Article 10 rights, for the reasons set out earlier.

se)? Should there, at least, exist a framework by which individuals can opt out of the personalised internet? These are questions to which we all may have no ready answers.

45. For many commentators, informed consent appears to be the answer. Some people will be happy for their data being disclosed. Others will not. That, however, raises the question as to what should be treated as informed consent. Is clicking the 'accept' button, acknowledging acceptance of the Ts&Cs, enough? I hazard a guess that, in this respect, few of us are like the late Sir Henry Brooke, of whom his son recently tweeted:

    '*My late father @HenryBrooke1 made a point of actually reading the terms and conditions accompanying software packages before clicking on 'Install'. I often wondered if he was the only person ever to do this, but I daresay it was second nature to him.*'[84]

46. The Court's approach so far has been that, for consent to be informed, it must extend beyond a mere understanding of what is taking place, to knowledge of an entitlement to refuse and the consequences of consenting[85]. In the context of Article 6, and the concept of waiver of the right of access to court, the Court has further explained that it must be free, unequivocal, and given in full knowledge of the facts[86]. In this regard, does the 'informed' aspect of consent require companies to explain everything in user friendly terms? As to the notion of 'consent' itself, account must also be taken of the situation on the ground. Who hasn't sought to resist downloading an update for an app or operating system only to discover that the app or phone is no longer functional without the update? If, with each update, we are asked to give our consent to the terms, can that still be described as a free and unequivocal consent? Similarly, if our lack of agreement to cookies, for example, prevents us from using an app or reading a particular website, is that still a true consent, even if informed[87]?

47. One answer may thought to be the development of alternatives performing the same function – Duck Duck Go, rather than Google, for example. However the operation of network effects, especially in relation to social media, may well prevent a generic website from performing the same function. If your network continues to use a specific social media app such as Facebook are we still able to exercise any meaningful choice?

[84] Michael Brooke (@marbleicehook), 14/11/2018, 22:03
[85] *Bože v Latvia* (no 40927/05), 18 May 2017
[86] *Suda v. the Czech Republic*, (no 1643/06) 28 October 2010; *Pfeifer and Plankl v. Austria* (no 10802/84) 25 February 1992
[87] The Council of Europe suggests in Recommendation CM/Rec(2012)4 (social networking) that 'the user's decision (refusal or consent) should not have any effect on the continued availability of the service to him or her'

48. Then we come to the problem of third parties. Take LinkedIn, for example, which offers the user the facility to import his or her email contacts to its servers to create 'links' on the site. Where it does, and harvests that data, are we in effect giving up the information of others for services they may well not have agreed to? How does this fit with their right to informational self-determination? If it is to be achieved for all, do we have to ask our friends in advance? To date, the line the Court has taken is to accept that we cannot always control the actions of our friends, but that it is our entitlement to consent to how our data is processed thereafter that matters. In *Muscio*[88],therefore, the applicant complained about obscene spam emails he had received. The Court held this complaint inadmissible. While receiving undesirable messages amounted to an interference with the applicant's private life, the nature of the internet meant that there was the inevitable risk of exposure to such messages. Consent may not, therefore, be a total answer to this problem.

IV. Where next?

49. Let us consider if there are other tools in the Court's jurisprudence which may enable us to answer some of these questions.

A. Positive obligations and private corporations

50. The potential risks posed to human rights by big data I have identified are posed by private corporations, a matter which presents some difficulties for the Convention. As you know, the Court – in exercise of its jurisdiction under Article 19 – is primarily concerned with the obligations (in the first place, negative obligations) – of member States acting through their public authorities. Drawing on the obligation under Article 1 to 'secure for everyone' the rights in the Convention, the Court has however developed the notion of positive obligations on member States to ensure individuals are also capable of being protected against interferences with their rights by other private individuals[89].
51. As a matter of legal principle, the concept of positive obligations is only one of a number of ways in which the Convention could have been applied to private persons. One notable alternative was the doctrine of horizontal effect or *drittwirkung'*. Ultimately, however, the Court did not adopt that approach considering it not '*desirable, let alone necessary, to elaborate a general theory concerning the extent to which the Convention guarantees*

[88] *Muscio v Italy* (no 31358/03, 13 November 2007)
[89] *X and Y v the Netherlands* (1985) 8 EHRR 235, for example

should be extended to relations between private individuals inter se'[90]. Instead, it has preferred (in line with the approach taken by the UK Supreme Court in *McDonald*[91], for example), to limit itself to the notion of positive obligations[92].

52. In the Court's case law, positive obligations are most frequently expressed through a requirement to put in place and, where appropriate use, a legal – civil or criminal – framework. In the specific context of the internet, the Court has already had cause to consider the scope of States' positive obligations in *Delfi AS* – its first articulation of the concept of 'duties and responsibilities' arising out of Article 10(2) as applied to internet intermediaries, and States' obligations in that context. In relation to both the Court set a high bar. In relation to the company, the Court found that the '*duties and responsibilities'* of Internet news portals engaged when they provided, for economic purposes, a platform for user-generated comments taking the form of hate speech and direct threats. An even stricter threshold was set in relation to State liability: '*…the rights and interests of others and of society as a whole may entitle Contracting States to impose liability on Internet news portals… if they fail to take measures to remove clearly unlawful comments without delay, even without notice from the alleged victim or from third parties*…'.
53. While, therefore, *Delfi AS* provides precedent for a positive obligation on States to create a regulatory framework, it has equally sought to avoid imposing too onerous a burden. It was material, that *Delfi AS* was a commercial actor – unlike the NGO publisher in *Pihl*[93]. This factor therefore may well justify member States affording different levels of protection, under Article 10, to commercial and non-commercial actors in an internal legal framework; it is certainly a factor that would be relevant in any overall proportionality analysis.
54. Though States' positive obligations relating to data protection can also be derived from the case law relating to the use of the internet in the workplace[94], those cases, have been largely confined to the employment context, with the Court emphasising the '*mutual trust*' underlying employment relationships (which is likely to be absent elsewhere).

[90] *Vgt Verein Gegen Tierfabriken v. Switzerland* (no 24699/94, 28 September 2001)
[91] *McDonald v McDonald* [2016] UKSC 28; see, most recently, *F.J.M. v. the United Kingdom* (dec.) (no. 76202/16, 6 November 2018)
[92] Although *Khurshid Mustafa and Tarzibachi v Sweden* (no 23883/06, 16 December 2008) is to be noted as an exception in this context
[93] *Pihl v Sweden* (no 74742/14 , 7 February 2017)
[94] In particular, *Barbalescu*. The Grand Chamber recognised that while States have a wide margin of appreciation in assessing the need to establish a legal framework governing the conditions in which an employer may regulate electronic or other communications of a non-professional nature by its employees in the workplace, the State must have regard to the principle of proportionality and provide procedural guarantees against arbitrariness. A number of employment-specific factors were set out in the Court's decision.

Beyond this, though, the Court has thus far had little occasion to grapple with how to draw the line in relation to States positive obligations in the realm of big data.

55. We must, therefore, return to first principles. In relation to Article 8, there is already an obligation to create a framework to reconcile freedom of expression and confidentiality of internet services with the protection of the rights and freedoms of others[95]. It may extend to an obligation to have and enforce criminal sanctions for 'grave acts', or civil sanctions for those less so[96]. Special protections must be afforded to vulnerable groups, in particular children.As a result, as and when States decide that the unregulated environment in which big data largely operates is in need of some regulation, it may need to include a (quasi-) judicial framework for the adjudication of disputes between individuals and the big data companies involved (such as applications under the right to be forgotten[97] or for content removal).[98]. Presently, limited information is available on how the process of content removal and/or de-linking takes place, less still whether requests are considered in accordance with Convention principles, making it difficult to guarantee accountability, transparency or due process. For these reasons, there may come a stage where it no longer suffices under the Convention for States to leave these matters to industry alone[99].

56. Similarly, in relation to Article 10, having regard to the kind of expression rights at stake, their capability to contribute to public debates, the nature and scope of the restrictions on expression, the availability of alternative venues for expression, and the weight of countervailing rights of others or the public[100], can is be said that States are responsible for creating an online environment in which everyone can (in principle) participate? The case of *Dink*[101], may be said to support such a suggestion, the Court finding that the State was required to create a favourable environment for participation in public debate, enabling individuals to express their opinions and ideas without fear,. Similarly, *Aksu v Turkey* (no 4149/04)[102] suggests that there may be obligations to protect vulnerable

[95] *K.U.*
[96] *Soderman v Sweden* (no 5786/08, 12 November 2013)
[97] An approach that would be equally merited under Article 10
[98]From the CJEU's decision to February 2018, Google received 748,008 requests for removal of a total of 2,864,297 URLs, of which 43.8% were removed – a sum of 906, 799 removed links https://transparencyreport.google.com/eu-privacy/overview?delisted_urls=start:1401321600000;end:1519862399999&lu=delisted_urls (Last accessed, 26 November 2018)
[99] The responsibility of the State may equally be engaged as a result of failing to enact appropriate domestic legislation (*Vgt Verein gegen Tierfabriken v. Switzerland*, no. 24699/94)
[100] *Appleby v UK* (no. 44306/98. ECHR 2003-VI)
[101] *Dink v Turkey* (no 2668/07 and 4 others, 14 September 2010)
[102]The applicant did not win on the facts but the Court confirmed that there exists positive obligations to protect individuals belonging to ethnic monitories from being subject to negative stereotyping. The Court said it may be considered necessary in

groups from negative stereotyping. Finally, thus far, the suggestion of a positive obligation on the State to disseminate public interest information of its own motion has been rejected by the Court[103], as has the suggestion of a rights based entitlement to use a particular website[104]. These are all areas to which it is likely the Court will be required to return in due course.

57. Let me just mention a few other issues and considerations more briefly.

B. Article 1 of Protocol 1 & the right to property

58. Beyond a simple recognition of their 'commercial interests' or 'for profit' nature in Article 8 and 10 complaints, thus far little has been said by the Court about the status of the private internet corporations themselves. They are of course capable of being rights holders in their own regard. The lack of jurisprudence has resulted in a considerable gap, in analysis and emphasis, which I cannot and do not remedy here. With a focus on the right to property, however, it is possible to identify some of the issues that may arise.
59. You will have noticed that, in the case law to date, the Court has tended to focus on data as an object which can be lost, acquired, sold, or consented away – each of which, Professor Alemanno suggests, reflects a European approach to data as private property[105]. But is this how data should be thought of? Or should it be treated as a public good because of its inherent value in informing interventions[106]? Professor Alemanno suggests that if data were treated as an essential facility akin to harbour or rail infrastructure, existing datasets could still be used (whilst being used by private companies) by either sharing the raw data or the observations from such data (though inevitably the terms of such data sharing and security would need to be carefully considered). The UN, in particular, appears to be exploring this idea further.
60. As an alternative, even if we do accept data is private property, could society approach (personal) data as something which can be licensed to others by individuals but over which the individual does not lose ownership? An analogy could be made with Apple Music or certain e-Books, to which we have a licence to for our lifetime post-purchase

certain democratic societies to sanction or prevent all forms of expression which spread, incite, promote or justify hatred based on intolerance provided that any formalities/conditions/restrictions/penalties are proportionate to the aim pursued.
[103] *Roche v the United Kingdom* (no 32555/96, 19 October 2005); see also *Magyar Helsinki* for an Article 10 example
[104] *Saliyev v Russia* (no. 25016/03) [2010] ECHR 1580. The Court noted that the State's obligation to ensure the individuals freedom of expression does not give private citizens or organisations an unfettered right of access to the means in order to put forward opinions.
[105] Alemanno, 2018
[106] As suggested in Alemanno, 2018

but which we cannot (it is thought) bequeath. If a company purchases or obtains data for commercial purposes and that data forms a part of the assets of that company, might lawful use (and holding) of the data (in general or for the public good) operate as a precondition of engaging Article 1? Even if not, might it be possible to argue that, say, the use of the data in the public interest constitutes (prima facie) a justified interference with Article 1? These points have yet to be explored in any detail albeit they are not – at least primarily – for the Court.

C. The precautionary principle

61. Is there room for application of a 'precautionary principle'[107] – a principally European concept providing that anticipatory action should be taken to prevent harm where a development may pose a risk to the environment or human health – to future developments in the technology sector? The principle has already been considered by the Court in the case law concerning scientific advancement generally, when identifying (as a part of the proportionality exercise) whether the interference was the least intrusive[108]. It may, however, require a shift in approach, if Professor Nemitz' view of the approach historically taken in the technology sector, as engineering driven and encapsulated by the phrase 'better to ask forgiveness than permission'[109], is correct. Nonetheless, taking artificial intelligence as an example, application of the precautionary principle may enable civil society, States and international organisations to answer complex questions before the technology is widely released, not least: (i) whether the meaning of personal data should change – might it include the '*uniqueness of body forms and movement patterns of human bodies'*[110]*?* ; (ii) whether to create a framework for liability for the actions of the artificially intelligent, answering (for example) whether it should be the driver or the manufacturer of a self driving car who should determine its settings and response to the trolley problem[111]; and (iii) ensuring any relevant State or international certifications are granted, and a legislative framework instituted beforehand.

[107] As defined by the 1998 Wingspread Statement on the Precautionary Principle
[108] See, for example, *Costa and Pavan v. Italy* (no. 54270/10, 28 August 2012). The judgment was determined by the principle of necessity, in so far as the test of the less intrusive measure envisages minimal impairment of the competing interests by asking whether there is an equally effective but less intrusive means available to further the same social need. In doing so, the Court also acknowledged the relevance of the precautionary principle in assessing interventions in the medical sphere, which aims at avoiding more severe interventions in favour of less severe ones at all stages of human life
[109] Nemitz 2018
[110] Nemitx 2018
[111] Wikipedia (https://en.wikipedia.org/wiki/Trolley_problem)

D. The protection of democracy

62. Professor Nemitz, in his paper, postulates unregulated big data as a fundamental threat to liberal democracy as we know it. In this context, it may be worth emphasising that the Council of Europe and, within it, the Court have – since their inception 70 years ago next year – always seen it as their fundamental role to protect the fundamental concept of a democratic society based on pluralism, tolerance and broadmindedness; a concept which is not solely majoritarian but provides and requires fair and proper treatment of minorities[112]. In exercising its function as guardian of the Convention and its underlying principles, the Court has always made clear that its protection extends beyond regulation of public authorities exercising their powers in a way inconsistent with the Convention, but extends to the protection of society from private actors seeking to fundamentally undermine democracy; even if apparently with the support of a majority in a member State (such as in *Refah Partisi*[113]).

E. The Court's jurisdictional limits

63. It is, of course, a defining feature of the internet that data disrespects borders. Traditionally, however, the Convention has by definition looked primarily to State borders to define its jurisdiction, tending to refer to national Courts' own assessment of jurisdiction[114] or taking a strictly State-focussed approach itself[115]. This can work in an applicant's favour if jurisdiction is found, as in *Perrin*[116] (in which a French national living in the UK, posted content on a website owned and operated from the US). The Court, there, accepted the Court of Appeal's rationale that an inability to prosecute could lead to publishers 'forum shopping' (publishing materials in the State with the lowest bars to publication) unless each Court was capable of taking action as to publications within its jurisdiction. By contrast, in the more recent case of *Tamiz*, concerning an applicant allegedly libelled in a blog run by Blogger (whose ultimate owner is Google) whose application was dismissed by the Court of Appeal on the grounds that he had not made out sufficient prospects to justify service of Google abroad, the application was found

[112] Y*oung, James and Webster v the United Kingdom* (nos 7806/77, 7601/76,), which concerned the State requirement for a particular trade union membership as a precondition for employment with British Rail; see also *Handyside*

[113] *Refah Partisi (the Welfare Party) and Others v. Turkey (no 41340/98, 41342/98, 41343/98, 13 February 2003),* concerning the imposition of a two-tier Sharia law system in Turkey which the Court rejected, finding the model of sharia advocated incompatible with the fundamental principles of democracy and divergent from Convention values.

[114] See, for example, *Pihl* in which the domestic Courts accepted jurisdiction in relation to the adjudication of a dispute between the applicant and the NGO posting the blog concerning him.

[115] Including where the member state exercises effective control in a third State: *Al-Skeini v UK* (no 55721/07 [2011] ECtHR)

[116] *Perrin v the United Kingdom* (no 5446/03, 18 October 2005).

inadmissible by the Court[117] on the grounds there was no error in the national Court's decision.

64. These cases may be said to demonstrate the limits of the Court's jurisdiction, which are likely to be tested by the internet.

V. Conclusion

65. New challenges arise at increasing pace, whether from 'deep fakes' – digitally generated videos using our faces and voices, and of sufficient apparent authenticity to make us appear to say and do things we did not[118] - or artificial intelligence in our homes[119]. While there has so far been only limited jurisprudence from the Court directed at addressing the issues raised by big data, throughout its history the Court has demonstrated its ability to develop its established jurisprudence to meet new challenges. In doing so, the Court has shown itself willing and able to act both as the guardian of the fundamental principles underlying the Convention, as well as the rights enshrined therein while seeking to facilitate (or at least not hinder) both technological and societal developments within the limits of their – in this context almost inevitably wide - margin of appreciation.

66. While we are no doubt confronted by significant new challenges arising in the context of big data, they should not be seen as insurmountable. Lorena Jaume-Palasí, the Executive Director of AlgorithmWatch and a member of the Spanish Government's Expert Panel on Artificial Intelligence and Big Data, suggests the following analogy: in the 1920s the question of liability for motor cars was hotly debated with leading critics deeply concerned about who would be held responsible and how far these new developments should be able to go (and how fast)[120]. The last phase of rapid industrial development around the same time led to the confluence of power in a few hands, and consequently to American and European competition and anti-trust law[121]. At the initial stages of both developments, there were uncertainties about how to proceed. Both demonstrate that it is possible to solve the problem of the integration of man and machine.

67. Returning to Sir Thomas More and his work Utopia, scholars have debated whether, in naming the island of Utopia, More intended to reflect the Greek *eu-topios* – a happy place, the land of perfection – or *ou-topios* – meaning nowhere, a place that does not

[117] *Tamiz v United Kingdom* (App No 3877/14).
[118] https://www.theguardian.com/technology/2018/nov/12/deep-fakes-fake-news-truth
[119] Perhaps Siri and Alexa could be construed in this way?
[120] See, for example, https://algorithmwatch.org/en/dont-fear-ai/
[121] https://www.theguardian.com/commentisfree/2018/nov/20/facebook-google-antitrust-laws-gilded-age

exist. I hope, this evening, I have been able to show that, as far as the Court is concerned, there is no reason why our course should not be firmly directed towards the former.

68. Thank you.

27 November 2018