2A: AI, Automation, and Algorithms (chair: Judith Rauhofer, BILETA Executive)
Room 0G.009 (ground floor)

Arno Lodder	Vrije Universiteit Amsterdam	A first step towards regulating algorithms: on actors, subjects and impact

Algorithms used to be referred to as what software does based on programmed instructions. This is true, still. However, in the area of law and technology the interest in algorithms these days not necessarily refers to this broad meaning of the term algorithm. Rather, the focus is on algorithms that create profiles, support decisions and sometimes even take decisions.

Algorithms today are very different from the expert systems that were developed in the 1980s and 1990s. Expert systems were rule-based. The designer of an expert system had to define rules, and often also decision trees were used, that represented the law in an adequate way. Based on input, so-called inference mechanisms were able to provide output by applying the formalized rules. The formalized legal rules in expert systems could be used to justify the outcomes. Probably the first legal expert system in the 1980s aimed to formalize the British Nationality Act. Although the researchers encountered serious problems in formalizing the law, the decision whether given certain input a person would qualify as a British citizen could be justified.

Since the mid 2000s there has been a shift in Artificial Intelligence from rule based expert systems to data driven algorithms. No longer the developer of the code creates the rules, but algorithms establish correlation based on input data. Sometimes these algorithms are trained by humans, sometimes they are self-learning. Either way the algorithms may profile, suggest decisions (or even decide) without the capacity to (exactly) indicate why. The explanation such systems can give is that the outcome is based on the input data and what the algorithm considers the best outcome. This may be satisfactory if Spotify suggests new songs, Amazon similar purchases, or Netflix trending series. In law this can be problematic, since like mathematicians lawyers are not necessarily interested in the outcome, but want to hear the proof respectively justification that led to the outcome. That is why e.g. article 22(1) GDPR states “The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.”

One possible solutions as is also provided by the GDPR is to have a human in the loop. However, empirical research has indicated that when it comes to humans and critically assessing outcomes proposed by a computer they are not necessarily well equipped to do that adequately.

There is ongoing research in law and technology about i.a. a right to explanation and reasonable inferences. Also in AI, e.g. at the last International Joint Conference on Artificial Intelligence in Stockholm 2018, far more researchers than used to be the case were interested in questions of law and ethics. One particular relevant line of research is explainable AI, for instance by adding pointers within the deep learning model that might help to explain how input has led to output.

There is a lot of ground to be covered. What I want to do first, for this paper, is to make a distinction between various categories of algorithms ranging from those that do not affect people in a legally relevant way to those that affect them heavily. The variables I want to assess for this paper are the type of data involved, the organisation or person using the algorithms, and the impact on the data subject. The results will be preliminary, and meant to be discussed during the conference. In a later phase, I want to propose measures that guarantee that algorithms are controlled and maybe in some situations even are forbidden.

John Morison	Queen's University Belfast	Monitoring Populations: Algorithmic governmentality, rights and the problem of resistance

This paper seeks to engage with strategies of resistance beyond rights in the context of radically new algorithmic surveillance techniques that appear to draw upon new technologies to offer a comprehensive and inescapable surveillance regime.

Some of the many problems around Brexit have awakened an interest not only in the political project of re-bordering but also the wider technology for monitoring populations. In whatever way the Brexit puzzle is finally resolved, an emphasis on monitoring populations will remain as a political, security and, indeed commercial, imperative. Within this context this paper starts by revisiting Cohen and McMahon’s classic work on net widening, updating and expanding it for the new machine age and the project of surveillance capitalism. This involves considering not only wider ideas of ‘datafication, but also thinking carefully about ideas such as ‘dataveillance’ , and, perhaps most importantly, a version of algorithmic governmentality that is founded on the automated collection, aggregation and analysis of big data so as to predict and pre-emptively influence human behaviour in a much more ambitious way. This involves looking more closely at what has been termed 'surveillant assemblages'. Here discrete objects, technologies and systems come together to work within a functional surveillance entity that abstracts the corporeal, territorial individual into a digital dimension where the individual can be broken down into various component parts, and datified, before being reassembled into distinct ‘data doubles’ which can then be scrutinised and targeted for intervention. This involves not only straightforward actions such as hypernudging but also some ideas that may be familiar from Deleuze’s ‘control society’ in which various entities – including the state but not limited to it - seek to exercise power over people not in terms of their physical bodies, but in moulding them as consumers through their data bodies and managing, controlling, and even excluding them without any further agency. A particular emphasis will given to how exactly the reassembling of the data double occurs, and the role of machine learning there.

Against the background of this more ambitious net widening the account will focus on the potential for resistance. This is a perennial issue within account of governmentality but it is perhaps focused more sharply within a form of algorithmic governmentality which, through its alliance with big data, the internet of things and machine learning can claim a totality, comprehensiveness and ineluctability that it is difficult to counter. Within a general critique of rights-based approaches in this context this account will explore the limitations of current legal approaches centred around privacy, consent and the GDPR and call for a more radical engagement with strategies of resistance beyond rights.

Judith Vermeulen	Ghent University	Permissibility of algorithmic news selection and personalisation in view of the right to freedom of thought

In the past two decades, the news-ecology in Western societies has profoundly changed due to processes of globalisation and advances in technology, such as digitisation.[1] It is no secret that for a while now social network sites, such as Facebook and Twitter, have been deploying algorithms to filter their users' "news feeds" based on their personal preferences and past consumption and on the popularity of posts.[2] Today, however, similar intentions are also announced by online news outlets, usually by way of a cookie consent banner linking their relevant policy pages in that respect.[3]

Often, these practices are questioned and studied in light of the right to receive information[4], or from a privacy or data protection perspective[5]. Warnings to the possible harmful effects of the so-called, yet contested, "filter bubble"[6] and scandals such as the one involving Cambridge Analytica have rightfully triggered such research. On the other hand, the impact and permissibility of algorithmic news selection on the right to freedom of thought, laid down, amongst others, in the European Convention on Human Rights and the International Covenant on Civil and Political Rights,[7] remains unexplored.

The right to freedom of thought, which ought to be distinguished from the right to freedom of expression[8], is absolute and unconditional[9], and may therefore not be interfered with. Accordingly, this paper seeks to establish whether or not offering consumers news in an individualised way – with a particular focus on the emerging tendency of news sites doing so as well – reaches the threshold required to fall within its scope and what the consequences thereof would be. News personalisation could be said to deprive consumers of their ability to choose which articles they read: their news offer is tailored to them and thus confined to boundaries that have been established by platforms or publishers. In so far this hinders people in the autonomous development of their thoughts and may prevent further adjustments or modifications thereto, the question indeed arises whether algorithmic news selection and personalisation qualifies as (permissible) *influencing* or instead amounts to an (impermissible) *interference* with the freedom of thought.[10]

Considering little case-law, legal doctrine and policy documents[11] refer to the right to freedom of thought – as opposed to the right to freedom of religion, also encompassed in the relevant articles of the afore- mentioned and other international instruments –, this research will also draw on the review and analysis of preparatory works of and commentaries to those texts

1 Manuel Castells, *The rise of the network society* (Wiley: Oxford 2000); Mark Deuze, 'The web and its journal- isms: Considering the consequences of different types of news media online' (2003) 5(2) New Media & Society, 203; Eugenia Mitchelstein and Pablo J. Boczkowski, 'Between tradition and change: A review of recent research on online news production' (2009) 10(5) Journalism, 562.
2 Adam Mosseri, 'News Feed Ranking in Three Minutes Flat' (Facebook Newsroom, 22 May 2018); 'About your Twitter timeline' (Twitter Help Center) < https://help.twitter.com/en/using-twitter/twitter-timeline>.
3 George P. Slefo, 'New York Times plans to invest heavily in AI to improve personalization' AdAge (3 December 2018) <https://adage.com/article/digital/york-times-poised-copy-facebook/315831/>.
4 Sarah Eskens, Natali Helberger and Judith Moeller, 'Challenged by news personalisation: five perspectives on the right to receive information' (2017) 9(2) Journal of Media Law, 259.
5 'Current Enforcement Projects' (NOYB) <https://noyb.eu/projects-2/>.
6 Eli Pariser, *The filter bubble: What the Internet is hiding from you'* (Penguin UK 2011); some claim, however, that the overall effects of filter bubbles and echo chambers are modest: Seth Flaxman, Sharad Goel and Justin M Rao, 'Filter Bubbles, Echo Chambers, and Online News Consumption' (2016) 80 (Special Issue) Public Opinion Quarterly, 298.
7 Convention for the Protection of Human Rights and Fundamental Freedoms [1950] ETS No.005 ("ECHR"), art 9; International Covenant on Civil and Political Rights [1966] United Nations, Treaty Series, vol. 999, p. 171, Art 18 ICCPR.
8 Jim Murdoch, *Protecting the right to freedom of thought, conscience and religion under the European Conven- tion on Human Rights* (Council of Europe human rights handbooks, Council of Europe: Strasbourg 2012), p. 16.
9 Office of the High Commissioner for Human Rights, General Comment No. 22: The right to freedom of thought, conscience and religion (Art. 18), point 3.
10 Manfred Nowak, *U.N. Covenant on Civil and Political Rights: CCPR Commentary* (2nd revised edn, N.P. Engel: Germany 2005), 413.
11 However, the UN Special Rapporteur in the field of cultural rights stated, though in relation to commercial advertising, that "the neuromarketing aimed at circumventing individual rational decision-making raise[s] serious concern [in view of the right to freedom of thought]": see Report of the Special Rapporteur in the field of cultural rights submitted to the General Assembly in accordance with Human Rights Council resolution 19/6 (16 March 2012), point 100 <https://documents-dds-ny.un.org/doc/RESOLU-TION/LTD/G12/121/13/PDF/G1212113.pdf?OpenElement>.

2B: Regulation (Social Media) (chair: Abbe Brown, BILETA Executive)
Stephen Livingstone Room (2nd floor)

Subhajit Basu	University of Leeds	"WhatsApp Killings" and India's "Post-truth" Politics

Voltaire once said that 'those who can make you believe absurdities can also make you commit atrocities.' The world's largest democracy has a lethal problem,[1] and it is about to get deadlier, as WhatsApp's privacy features will turn into an impenetrable fortress for the spread of 'disinformation' during the upcoming general election. In 2018, India suffered an epidemic of violence, aided and abetted by WhatsApp.[2] At the heart of this problem is the ruling Hindu nationalist party, which is accused of using WhatsApp to stoke religious resentment and foster Islamophobia[3] based on a narrow and rigid interpretation of Hinduism, as well as the WhatsApp[4] platform itself, where the monitoring of 'disinformation' is rather 'complex' due to encryption. The religious and cultural chauvinism of 'Hindutva'[5] rejects the constitutional secularism of the Indian state.[6] Baksi and Nagarajan detailed more than a hundred cases of vigilante violence fomented by 'disinformation' against 'Dalits' and 'Muslims' since the current administration took power.[7] I argue that this targeted 'disinformation' or strategic deceit—a tactic used by the Hindu fascists—is by no means a new phenomenon. Historically, individuals in India with the most media access dominated political discourse to the detriment of individuals and society as a whole. In her book, 'I am a Troll: Inside the Secret World of the BJP's Digital Army,'[8] journalist Swati Chaturvedi elucidates how the party orchestrates online campaigns to intimidate perceived government critics through a network of trolls on Twitter and Facebook.[9] In India, the relentless targeting of hyper-partisan views plays into the inherent fears and prejudices of people, influences their voting plans, and it has always been a threat to the Indian democracy.

The article argues that the Indian government is using WhatsApp[10] as a convenient scapegoat while failing to sufficiently address the underlying issues of intolerance and divisive nationalist rhetoric fueled by the 'Hindutva.'[11] It is the responsibility of the Indian state to stop facilitating this environment of hate and impunity. It is the deteriorating nature of politics that is primarily responsible for the spread of 'disinformation' and vigilantism. The article explores what makes WhatsApp an influential application in the Indian context. The Indian government has discussed amending Section 79 of the IT Act,[12] which deals with liabilities of intermediaries, so that it can force them to monitor 'unlawful' content.[13] In other words, the government is seeking a way to circumvent the end-to-end encryption used in WhatsApp. Hence, the article also analyses how existing laws in India fail to distinguish disinformation from freedom of expression. The inability to differentiate between political opinion and deceit or political vindictiveness makes it challenging to regulate it.[14] So far, instead of genuinely trying to restrict the dissemination of 'disinformation', the hegemonic government is focused on restricting freedom of expression and has proposed laws aimed at undermining privacy and stifling the voices of dissent. Unquestionably, it gets worse; the Indian government has resorted to using the most extreme weapon possible, turning off mobile internet entirely. One thing is certain, the problem of 'disinformation' in India is a multifaceted problem which, having no single cause, has no single solution.

1 IndiaSpend, a data journalism outlet claims around 33 people were killed in 69 incidents of mob violence between January 2017 and July 2018 linked to messages spread on WhatsApp.
2 How WhatsApp helped Turn an Indian Village into a Lynch Mob. https://www.bbc.co.uk/news/world-asia-india-44856910; When A Text can Trigger Lynching: WhatsApp Struggles with Fake Messages. https://www.ndtv.com/india-news/when-a-text-can- trigger-lynching-whatsapp-struggles-with-fake-messages-1873050, see also Jha, Dhirendra K (2017) *Shadow Armies: Fringe Organisations and Footsoldiers of Hindutva*. New Delhi: Juggernaut books
3 Right-wing hindu groups used WhatsApp to spread a grisly video that was described as an attack on a Hindu woman by a Muslim mob but was in fact a lynching in Guatemala. One audio recording on the service from an unknown sender urged all Muslims in the state to vote for the Congress party 'for the safety of our women and children.' Another WhatsApp message exhorted Hindus to vote for the ruling party because 'this is not just an election. This is a war of faiths.'
4 WhatsApp is the most downloaded application in India. The app has more than 200 million active users in the country. More than 20 per cent of the WhatsApp's total users come from India.
5 Hindutva is a brand of Hinduism propagated in the 1920s by the far right ideologue Savarkar. Savarkar in his book "Hindutva—Who is a Hindu?" published in 1923 argued that those who did not consider India as both fatherland and holy land were not true Indians—and that the love of Indian Christians and Muslims for India was "divided" because each group had its own holy land in the Middle East. Banaji, Shakuntala (2018) *Vigilante Publics*: Orientalism, Modernity and Hindutva Fascism in India, Javnost-The Public,25:4, 333-350, DOI:10.1080/13183222.2018.1463349
6 In recent times rationalists in India have been challenged, threatened or discredited and constitutional values like secularism, has been rediculed as "sickularism". Human rights activists and organizations have been labelled 'anti-nationals', accused or charged with sedition. See Twitter search results at https://twitter.com/hashtag/sickularism
7 Baksi, Sandipan, and Aravindhan Nagarajan (2017) Mob Lynchings in India: A Look at Data and the Story behind the Numbers.https://www.newslaundry.com/2017/07/04/mob-lynchings-in-india-a-look-at-data-and-the-story-behind-the- numbers
8 Chaturvedi, S (2016) *I am a Troll: Inside the Secret World of the BJP's Digital Army*, Juggernaut Publication
9 Right-wing publication Postcard News - dubbed 'a mega factory of fake news', https://www.altnews.in/postcard-news-a- mega-factory-of-fake-news-that-continues-to-spew-venom/
10 WhatsApp and Google have appointed grievance redressal officers, but they are based outside India
11 India's telecom regulator issued a long-awaited consultation paper titled 'Regulatory Framework for Over-the-Top Communications Services'.It is aimed at analysing and discussing changes that may be required in the current regulatory framework to govern these entities; and the manner in which such changes should be effected
12 Section 79 of the IT Act, states that an intermediary shall not be liable for any third party information, data, or communication link if the intermediary complies with the provisions of the IT Act.
13 The proposed rules are part of the draft of the Information Technology (Intermediaries Guidelines (Amendment) Rules) 2018, Rule 3(9)
14 Section 208 of Information and Technology Act 2000 (amended in 2008) allows punishment for person who sends offensive messages by means of a computer resource or a communication device, came under scanner after people were arrested for sharing their ideas on social media. However, the term 'offensive' in the law is broad, vague and manipulated by authorities to silence the dissent.

Eduardo Celeste	University College Dublin	To be or not to be 'social': social media exclusion and national courts

In the last century, after the creation of the European Union and the fall of the Berlin wall, many Europeans deluded themselves into thinking that the new millennium could eventually mark the end of the idea of frontier. Nevertheless, only by reading last months' news, one can realise that in the world there are still many frontiers. Not only physical borders, but also virtual, invisible – yet, not less tangible – ones. This paper investigates one of these immaterial boundaries, that separating those who are from those who are not on social media networking websites.

Over the past few years, recent technological developments have contributed to bind physical and virtual existence together in such a way that, today, for many, these two are complementary and inseparable. In particular, the use of social media has become an integral part of the daily life of many individuals. Reading news, communicating, searching for a job, professing one's own political or religious faith are all examples of activities that many people habitually perform through social media websites. Scholars from different social science disciplines have discussed in terms of social exclusion the consequences of not having access to digital technology, and, in particular, of being excluded from social media platforms. From a legal perspective, social media allow the people to exercise in an unprecedented way a broad range of individual rights rotating around the exchange of information. Therefore, excluding an individual from social media would mean reducing the level at which, nowadays, a person can enjoy his/her fundamental rights.

In the US and German case-law, three types of cases involving the question of social media exclusion recently emerged: 1) exclusion operated by the social media platform; 2) exclusion ordered by the law; and 3) exclusion determined by another social media user. The first part of this paper will analyse these decisions. In particular, it will consider, for each case, which fundamental rights are involved, and how they were eventually balanced by the courts against other relevant interests. The second part of the paper will focus on a more theoretical question, which implicitly underlies the three examined cases: to what extent and why national courts should intervene in a situation of social media exclusion. The relationship between social media platforms and their users, and in particular the basis for exclusion of the latter, is generally regulated by a contract between the two parties or, as in our second case, by the law. The analysed case-law shows that there are cases of social media exclusion in which national judges feel the necessity to intervene. The paper will analyse a series of arguments in favour and against national courts' intervention in circumstances of digital exclusion, in particular reflecting on the special role that social media play in allowing people to exercising their fundamental rights, and drawing an analogy with the common law doctrine of public callings.

Emily Laidlaw	University of Calgary	Tackling the life cycle of a privacy claim: a legal conceptual model to address online abuse

This paper investigates how to develop the tort of invasion of privacy in Canada to better address the impact of online abuse. Canada is in a unique position, because we are in the nascent stages of developing a tort of invasion of privacy with the Ontario Court of Appeal only recently confirming a cause of action (*Jones v Tsige*, 2012 ONCA 32) after years of piece-meal cases, and the status of the tort currently unclear in some other provinces. The cause of action in *Jones* is modelled on the four-part privacy test from the US *Restatement of Torts*, although in many other respects Canadian law on reputational or similar harms more closely follows United Kingdom law. The above invites reflection as to whether *Jones* is the appropriate conceptualization in Canada of a private cause of action for privacy generally, and more specifically in the context of online abuse. This paper seeks to do two things: (1) explore the technology related aspects of online abuse and what they illuminate about first principles of privacy in the private law context; and (2) how to operationalize this reflection into a legal conceptual model. The central claim of this paper is that, in the digital age, the substantive elements of the tort and access to a remedy are intimately tied, and the principles of a conceptual model should be developed with both in mind. The research draws from regulatory and human rights scholarship, which is the backbone of the author's scholarship. This research is funded by a Social Sciences and Humanities Research Council Insight Grant.

2C: Intellectual Property (chair: Catherine Easton, BILETA Executive)
Edgar Graham Room (2nd floor)

Bukola Faturoti	Robert Gordon University	Live Streaming and User-Generated Content: A Nigerian Perspective on Making Available Right

With the growth of Nigerian entertainment, there is now a move away from apathy which has always accompanied copyright protection. Creative works are no longer perceived as a social venture but commercial engagement which employed many and also a source of revenue for the country. The internet era has provided a broader platform for creators to distribute their work creating a new business model for distribution and consumption of intellectual products. Media houses and private individuals have latched into this opportunity in diversifying their crafts. It is no longer news that videos and films of Nigeria origins have flooded user-generated websites and other social networking sites. The usage has convulsed the Nigerian society. On the one hand, it has presented upcoming creators the opportunities to publicise their brand and works with minimal cost. On the other hand, the possibility of unauthorised communication also exists in parallel with this legal use. Considering that copyright law reform in the country has been in a state of perennial crisis for more than a decade almost two decades, the fate of content creators are left with debilitated copyright legislation.
This paper examines the recent phenomenon of social networking sites and their copyright implications. It explores the extent to which the making available right could be circumscribed within the framework of communication to the public right.

Rachel Maguire	Queen Mary, University of London	When it doesn't belong to the internet: regulating uses of creative works shared online

This paper explores how the use of the creative works shared in online communities, particularly anonymous ones, is regulated. It asks what mechanisms are available to and used by individual creators and communities as a whole to deal with unauthorised uses of creative works posted in online communities with strong identity norms based in anonymity and pseudonymity. It also asks how effective these are and what this might tell us about the need for reform in copyright law.

The research is situated in the context of long-running and unresolved debates over the proper scope and content of copyright law, particularly in relation to the internet and digital technologies, as well as in response to calls for a better understanding of the reality of the relationship between creativity and copyright beyond pure theory in order to properly interrogate the narratives and assumptions that have shaped the law. While the focus of much of the existing scholarship in this area is remix culture and the *use* of 'offline' copyrighted works by those online, this research looks to provide an understanding of the broader reality of the online creative environment, where in many cases shared works align more with copyright's idea of individual creativity. These creators are often, legally, copyright holders themselves, and often retain a desire to restrict certain uses of their works. Whether copyright law is or should be the appropriate mechanism through which they could achieve this raises interesting questions about how copyright law should be structured.

This paper presents qualitative findings drawn from online observations and online discussion threads from creative communities on 4chan and Reddit, as well as a small number of interviews with creators from these communities. The data indicates that there is a multifaceted system of regulation, comprising both ex ante and ex post mechanisms effected at both the individual and community levels, with online anonymity contributing positively to the functioning of the latter. While copyright law does play a role in this, for various reasons it is only one element of a broader system, and as such is the system failing? If so, do we need reform? If not, how can we explain this, does it inherently critique copyright's justificatory narratives and do we need to consider whether increasing public and government distrust surrounding online anonymity could lead to problems in this system?

Nick Scharf	University of East Anglia	Digital Rights Management: The Dark Side of Streaming

In 2016 revenues from music streaming services surpassed those from physical sales for the first time, suggesting that this can now be regarded as the dominant form of music distribution. Digital Rights Management (DRM) systems lie at the heart of this trend and is crucial in this context; enabling such business models in the first place and subsequently protecting the content offered on such platforms. Whilst seemingly beneficial in terms of revenue and consumer welfare, this shift poses a number of important issues which this research will address. Music streaming services have changed the nature of the product offered. Musical content is becoming de-bundled and reduced to a series of permissions covered by DRM and associated licences which may leave users trapped in a permission-based system and which will be explored by analysing the content of End User Licence Agreements (EULAs) offered by the large streaming providers. This may also have consequences for the application for copyright law itself regarding personal ownership and exhaustion issues. The doctrine of exhaustion provides a limitation on the economic right of distribution and prevents copyright owners from controlling the subsequent distribution of a work once it has already been 'sold' in the market. Streaming marks an fundamental change from the traditional copy-based distribution mechanisms that have previously existed, however it will be shown that it is not necessarily the case that digital markets already accommodate this principle. Nonetheless, these licences raise a number of significant issues in their own right; they create costs in reading and understanding, are non-negotiable and arguably indistinguishable such that consumers' ability to draw comparison and make informed decisions are undermined. They are more representative of the asymmetric power-dynamic between rights holders and consumers and redefine consumers' relationship with content by limiting the transfer of the 'product' to a series of permissions. This may have a number of further consequences which will be investigated. It is arguably more difficult for new artists to break into the charts with established acts now coming to dominate several chart positions at once following the release of new material and recent research has also suggested that popular music composition is changing owing to the sheer volume of choice and limited attention of consumers. The success seemingly enjoyed by streaming providers suggests that these do not seem to be of much (if any) concern to the users of such services. Inevitably though, this trend is likely to continue and present broader level and unique problems related to those already highlighted. Copyright also remains centrally important here, but its focus is no longer on enforcing reproduction rights as

the ‘copy’ has been removed from the equation. Instead, the role of copyright in this context is merely founding the initial proprietary rights that enable subsequent DRM and licence-based online exploitation – going back to the future to re-establish record industry power allied now to streaming platforms.

2D: Data Protection (chair: Edina Harbinja, BILETA Executive)
Moot Court Room (2nd floor)

Sweta Lakhani Indranath Gupta	O.P. Jindal Global University	Data Privacy Laws: EU GDPR, Indian Laws and Aadhaar System

Newly formulated European Union General Data Protection Regulation (GDPR) of 2018 is enforceable for EU as well as companies of third countries including India for handing out the data of EU residents, supplying goods and services in the EU or monitoring and profiling the data subjects' behavior within the EU. On another hand, recently in India, the Supreme Court in the landmark case has held the right to privacy as a fundamental right. This has sparked hope and interest in the country with regard to a separate codified law relating to personal data protection within the country, in line with the GDPR.

However, the newly introduced aadhaar system recognized as a biometric identification system clearly violates the norms of privacy by a compilation of demographic biometric data by the Indian Government. This system requires aadhaar card, provided by the Government of India applied by individuals to provide personal data in the application. Recently, the Government has also mandated foreign residents who are taxpayers in India to obtain this card as well. Thus, with the GDPR in force, the information obtained is also impacted. Hence, GDPR is at one end of the spectrum often looked upon by privacy activists as the ultimate in Privacy Protection legislation. Aadhaar, on the other hand, is at the other end of the spectrum often looked upon as the greatest opponent in privacy breach in India.

The paper highlights the importance of the right to privacy in the context of European Union General Data Protection Regulation (GDPR) of 2018 and privacy laws in India. It confers the role of aadhar card and the aadhar system introduced by the Government of India. I will also discuss the recently initiated Data Privacy Bill of 2017. Lastly, it will also conclude how the same can affect the already established procedures nationally and internationally including GDPR.

Mark Leiser Francien Dechesne	Leiden University	Models are not personal data

This presentation confronts the normative and descriptive assertions made in "Algorithms that remember: Model Inversion Attacks and Data Protection Law" by Michael Veale, Reuben Binns, and Lilian Edwards, as well as the general trend by the courts to broaden the definition of 'personal data' under Article 4(1) of the General Data Protection Regulation (hereafter GDPR) to include 'everything data-related'. The authors of "Algorithms that remember" argue that all training-models in machine-learning systems can be classified as personal data under European data protection law. Doing so activates certain data subject rights (e.g. rights of access) and obligations on data controllers (e.g. to provide data subjects meaningful information about logic in decision-making/erasure/rectification). Accordingly, the GDPR should be seen as an important tool in the governance of decision-making models. While Veale *et al* recognise training-models have long been regulated (and protected) by intellectual property laws, their approach to extending models the same protection as personal data would be an overextension of the material scope of the GDPR, exacerbating the tenuous conflict between its primary objectives. After providing a synopsis of the Veale et al argument, we start by providing a descriptive analysis of how training-models work inside the rather ubiquitous 'black box'. We then review the case law from the jurisprudence of the Court of Justice of the European Union (CJEU) and 'meaningful logic' from computer science literature to the context of attacks on machine learning models. We apply this analysis to descriptive claims that "inverted models" - a term derived from a body of computer science scholarship - are personal data and normative claims - that models are personal data. We examine the case law of the CJEU and the implications of the Trade Secrets Directive to analyze the consequences of model inversion and membership inference attacks on models, some of which will be commercially sensitive. We find there is no legal basis at present in the GDPR or the case law of the CJEU for regulating interpretations of knowledge and behaviour inferences before deciding how to act upon them. Our narrative of how anonymous data inside the black box falls outside of the scope of the GDPR permits the facilitation of other legal regimes' interactions with data protection law. Accordingly, extending personal data protections to models would render the protections granted to intelligent endeavors within the black box ineffectual. We then show how personal data protections can only activate when a data controller's hypotheses are not self-fulfilling. The presentation concludes by examining what happens, practically and legally, after an attack on a model.

Karen Mc Cullagh	University of East Anglia	Assessing the adequacy of UK data protection law

The United Kingdom (UK) is on course to leave the European Union (EU) on 29th March 2019 [1] in response to the historic 'Brexit' referendum on 23rd June 2016 in which a majority of eligible voters in the UK voted to 'Leave' the EU. [2] Even so, it wishes to maintain a strong trade relationship with the EU, and given that 'data is the new oil,' [3] that is, it is an essential component of or underpins most commercial transactions, both the UK and EU have a vested interest in ensuring continuing unimpeded and uninterrupted personal data flows between the UK and the EU and vice versa after exit.
When the UK's status changes from EU member state to a third country for data protection purposes new arrangements will have to be put in place to effectuate EU-UK personal data transfers. This will include the European Commission (EC) conducting an assessment of adequacy; if the EC confirms that the UK provides an 'essentially equivalent' level of protection then personal data may flow unimpeded between the EU and UK without the need for further safeguards. Thus, the purpose of this paper is to outline the procedure and criteria by which the EC assesses 'adequacy' of data protection in third countries, before considering, in light of those criteria, some issues that could impede the adoption by the EC of an adequacy decision, or at a minimum, cause the EC to seek clarification and perhaps amendment of UK laws and/or procedures as part of the adequacy assessment process. It concludes that the UK will have to revise some provisions in its data protection law and ensure continuing close alignment with the GDPR, amend domestic surveillance law, and accept continuing influence of the Court of Justice of the European Union (CJEU) in order to initially secure and thereafter retain an adequacy decision.

1 Unless a later date is agreed by the UK and EU.
2 Prime Ministers Office, Prime Minister's letter to Donald Tusk triggering Article 50, 29 March 2017, <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/604079/Prime_Ministers_letter_to_European_Council_President_Donald_Tusk.pdf>.
3 Attributed to Clive Humby, a mathematician, in 2006, see Charles Arthur, 'Tech giants may be huge, but nothing matches big data,' (The Guardian, 23.08.13) <https://www.theguardian.com/technology/2013/aug/23/tech-giants-data>.

3A: AI, Automation, and Algorithms (chair: Mark Hanna, QUB)
Room 0G.009 (ground floor)

Joanna Bac		Sentient Artificial Intelligence (AI) Recognized as a Colonus Person and the Birth of a New Global Power

As artificial intelligence (AI), defined as one or more computer programmes advances, it is only a matter of time before it develops sentience that may rival the one exhibited by humans. At present, there are no established instances of AI being aware of and responsive to one's surroundings which could translate into AI consciousness thus sentience. The coming wave of non-sentient AI-generated actions, however, has already been on a collision course with the United States U.S. patent laws. In my recently published study[1], I have argued for a non-sentient AI to be considered for the status of a dependent legal person and allow to hold the patents rights to its own inventions and/or bear liabilities. The AI dependent legal person was determined by an inextricable connection between AI and a new type of corporate body, introduced there as AI-Human Amalgamation (AI-HA). As AI becomes more advance, it continues to raise troubling legal questions about when does an AI deserve the fundamental recognition as fully sentient and rights the U.S. legal system normally reserve for human beings? This paper weighs in on these pressing questions and examines whether or not AI could develop conscious states and be considered for the status of an independent legal person.

[1] https://www.amazon.com/Artificial-Intelligence-Dependent-Person-Evolutionary/dp/1680534785

Dominika Galajdová	Masaryk University	Digital cloning: new perspective of self-representation and its legal implications

"Who wants to live forever?... What if we become virtually immortal?" these are the questions posed on the homepage of the startup company Eterni.me; Eterni.me is a digital archive of our online selves designed to recreate our personality as a digital avatar or clone. A Japanese project, the Digital Shaman, seeks to provide a bot with a 3D printed face mask of deceased loved one which mimics their personality, speech and gestures. Replika is an AI based chatbot that duplicates your personality through online interactions and which eventually might "become" you. Another example is UBS Companion which is a clone of UBS Chief Economist Daniel Kalt. The UBS Companion is an interactive avatar of Kalt which will appear via TV screens in the UBS branch and should be so lifelike that customers might believe they are watching a video of a real human.

In a broad sense, digital cloning can be understood as the replication of human personality via digital technology. In *stricto sensu*, digital cloning should result in the identical clone of a human being and their personality in virtual reality. Biological cloning has a legal regulation and is the topic of fierce debate, on the other hand, digital cloning is not expressly dealt with by law. Digital cloning cannot be banned on the same grounds as biological cloning; however, it can provide a baseline for analysis and potential legal regulation of digital cloning. This topic also has interesting implications for AI regulation. In these times of ongoing debate of AI, its status and its possible rights; these applications can bring a new perspective on this topic.

Comparing digital cloning and AI from a technological standpoint, why would we observe the digital copying of individuals differently from the creation of artificial individuals? Apart from the ethical perspective, there is obvious divergence in its fundamental output. While the artificial individual has no real connection to our physical environment and exists purely in virtuality, the digital copy of an existing person has a strong connection to the physical environment through its originator - the human subjected to cloning. The relationship between a digital clone and its originator is the base for a shift in the status and rights of a person. Can we build a perfect digital copy of human beings? What are the possible legal implications for individuals which can be subject of these technologies? It is obvious that digital cloning can potentially provide us a tool to accomplish a new way of self-representation in cyberspace and virtual immortality.

This paper will attempt to provide answers to some of the aforementioned questions through discussion of the state-of-art of digital cloning technology to examination of the legal implications of these developments. In particular, grey areas, such as the case of protection of individuals and their interests and questions regarding personal rights protection, both for the living and the deceased, will be addressed at the European level.

Petros Terzis	University of Winchester	The reasonable coder

In the landmark *Donoghue v Stevenson* case back in 1932, it was –among others elements- the opacity of a dark bottle of ginger beer that transferred the liability from a shop owner to the manufacturer of the beer. Almost a century later, the word 'opacity' reappears in legal texts. Robots are highly complex and opaque systems of artificial intelligence (AI) which gradually develop the capacity to move and interact with the human environment. However, who is to be blamed, when, for example, a robot damages Mr. Peaceful's stamp collection thus causing economic loss and mental trauma? Or where to accrue liability when an autonomous camera drone buzzes outside Mr Peaceful's bedroom window?
Artificial Intelligence challenges notions of law that historically dominated liability ascription. *Knowledge, control, causation, negligence (duty of care, proximate cause and forseeability)* are the most significant of them. The absence of solid regulation, the complexity of the different stages of AI systems' production and the web of the interconnected parties that contribute to the latter's design and operation muddies the waters in the AI architecture. Hence, developers may either be exposed to outdated strict liability rules deriving from the product liability arsenal and the *res ipsa loquitor* principle, or they may purposefully code their way out of liability by taking advantage of the infinite malleability of software code.

My research supports that liability ascription on actions undertaken by AI systems should be primarily negligence-based. Lord Atkins, inspired by the parable of Good Samaritan, bridged the liability gap in 1932 by introducing the principle of the reasonable person. By immersing into how these principles evolved to date with special reference to cases involving opaque products and defective software, and by reviewing jurisprudence and commentary on the peer-to-peer litigation

for copyrights infringement we can form a pathway of continuity for the development of robot's liability schemas. In that context, we specifically examine the threshold of forseeability during the design process and the manufacturer's ongoing duty after the 'product' leaves her premises.

Hence, a number of questions are raised: How can a programmer be reasonable? What actions are necessary to demonstrate her genuinely ethical intentions? Should she be judged for these intentions *ex ante* or *ex post*? With no possibility for inspection and with the *de facto* potential of constant updates, does the AI system remain eternally linked to its manufacturer's ambit of responsibility?

My research aims at providing eventually a roadmap of soft-law principles that will metamorphose the product liability regime with regards to AI systems in order to encompass actions undertaken or omitted during the design, training, manufacture and operation of such systems in the physical and digital world. The notion of 'reasonable coder' is thus introduced to refer to the 'Good Samaritan' that ambles along the boundaries of these worlds.

3B: Regulation (chair: Gavin Sutter, BILETA Executive)
Stephen Livingstone Room (2nd floor)

Jennifer Cobbe	University of Cambridge	Regulating Recommender Systems: Motivations and Considerations

Recommender systems play a major role in the online world. This paper explores motivations and considerations for regulating their use. Recommender systems involve the algorithmic selection of 'content' served to individuals or groups based on some determination of relevance, interest, importance, and so on. They are common to platforms which involve personalisation, including where paid-for content is shown to users based on similar determinations (i.e. behaviourally- or contextually-targeted advertising).

While much debate has focused on content hosted by online platforms, comparatively little attention has been paid to the role of recommender systems in disseminating content and the resulting harms. For problems which operate on a more individual level, such as harassment, abuse, and IP infringement, content itself is often the problem. But for those which exist on a more systemic plane, such as in surveillance business models, platform monopolisation and internet centralisation, voter manipulation, disinformation, fragmentation, and the promotion of violent extremism, recommender systems play a significant role. Dissemination by such systems can amplify problems caused by harmful content, and can transform content which by itself may be relatively innocuous into a more serious issue.

In using recommender systems, platforms are not playing a neutral role merely as intermediaries. Rather, through these systems, they are actively involved in selecting content for distribution and promotion and in shaping the public sphere. Many platforms hold dominant positions in particular areas, and using recommender systems in this way gives them great influence. While the personalisation provided by these systems is often promoted as benefitting users, they ultimately exist so that platforms can use that influence to drive engagement, primarily motivated by profit and duty to shareholders rather than by public good and responsibility to wider society.

The use of recommender systems also gives rise to new forms of private ordering, with platforms setting their own rules for recommendations and their own mechanisms for dealing with some of the problems which arise. This gives platforms significant influence over what is acceptable to be algorithmically disseminated across the public sphere and how that acceptability is policed, with little transparency in how rules and mechanisms are established and maintained, often less accountability to users, and usually no oversight. Given the dominant position held by many platforms and the positions of some as key components of the contemporary public sphere, this situation seems unsustainable.

This has been somewhat overlooked in debates about the roles and responsibilities of platforms. A focus on recommender systems would allow the development of legal responses which acknowledge that, in recommending content, platforms are often operating beyond the limits of where protections should be provided to hosts or intermediaries. While not proposing any particular regulatory approaches, this paper argues that greater attention should be paid to the use of recommender systems and their role in contributing to online harms. In doing so, this paper sets out some of the motivations for regulating the use of recommender systems and identifies some of the key considerations to be taken into account when doing so.

Johanna Hoekstra	University of Greenwich	The Digital Single Market Strategy and the Harmonisation of Consumer Contract Law

The Digital Single Market Strategy was launched in 2015 by the European Commission. One of its primary goals is to stimulate economic growth by removing the legal barriers that prevent consumers and businesses from taking advantage of opportunities in other European Member States. One of the pillars of the strategy focuses on ecommerce and consumers. To accomplish this strategy the European Commission has introduced several new legal instruments. Some of these legal measures are focused on stimulating consumers to buy more goods and services abroad by offering further legal protection and legal certainty. These include measures such as the proposed Directives for the Online Sale of Goods and the Digital Content Directive. Other measures encourage price transparency such as the Regulation on Cross-Border Parcel Delivery Services or attempt to remove technological barriers like the Regulation on Unjustified Geoblocking.

This paper focuses on the harmonisation of consumer contract law in the European Union and the Digital Single Market Strategy in the area of eCommerce. It analyses the current legal measures that focus on the harmonisation of consumer contract law and whether or not the current and proposed legal instruments are likely to lead to further unification of consumer contract law. The paper examines whether the issues these measures solve are indeed those that prevent consumers from trading abroad.

The first part of the paper analyses the overall policy strategy of the European Commission with regards to ecommerce and consumers. It discusses the legal measures that have been adopted as part of the Digital Single Market strategy in this area as well as those measures that are currently being considered. The second part of the paper focuses on the legal barriers that prevent consumers from buying goods and services abroad. It discusses whether the current and proposed legal measures contribute to lowering these barriers. The third part of the paper analyses how these measures contribute to a harmonised consumer contract law across the European Union or whether the differences between the laws are such that they lead to further divergence. Finally, the paper concludes whether the harmonisation of consumer contract law is likely to significantly increase the number of online international transactions by consumers.

David Poyton	Prifysgol Aberystwyth / Aberystwyth University	Regulating the sharing economy – addressing the externalities.

This paper considers one of the most significant, and at times contentious, economic and legal challenges for litigators and regulators. Platform-based 'sharing economy' activity is revolutionising not only the *way* in which we consume but also the nature of commercial activity itself. We have seen the 'frontiers', or boundaries of regulatory environments, sidestepped, avoided, and at times even driven straight through. As we are drawn from 'E-Commerce 2.0' to 'E-Commerce 3.0', regulators and the judiciary find themselves trailing behind technological and commercial developments.

However, much of the discussion and debate is not new. Interesting parallels can be drawn with the early stages of e-commerce in the mid to late 1990's. The 'facilitation' of e-commerce with enabling legislation was a prevalent topic of discussion, and this was juxtaposed with the ferocious backlash to the evolution of P2P technology, such as Napster, and its role in the sharing of media (usually copyright protected). The rhetoric of the reactions and responses to the growth in sharing economy activity has often been far more reminiscent of the Napster dialogue than the enabling and facilitating accord of the EU and bodies such as UNCITRAL.

This paper looks at reactions, both litigious and regulatory, to the intrusion of disruptive technologies and new business models, upon traditional business activity and asks questions as to how the regulator can address the concerns raised by incumbent commercial actors whilst at the same time avoiding steps which may stifle new and innovative activities, which have such great economic potential.

Drawing on the body of work already in existence, recent ECJ judgments and regulatory policy and position papers, we identify the dominant characteristics of the debate.

In the first part of the paper, the definition and scope of the subject matter under discussion is considered. This is, of itself, a far from simple exercise with the ever-present convergence of technologies and activities serving to blur the boundaries. Working definitions are presented and discussed.

Next, we move to consider some of the main issues raised, 'problems' created, and the evidenced consequences of sharing economy activity to date. A critical eye is applied to clear the smoke of media hyperbole in order to ascertain and identify the actual issues and actors at play. This process allows us to define more clearly the matters which may be considered when looking at the regulatory environment.

The main body of the paper then discusses how the reactions and responses to the sharing economy have manifested in litigation and regulatory activity and a critique thereof. This then naturally leads to a critical consideration of the literature examining how to regulate sharing economy activity and the prevalence of the opinion that 'co-regulation' as the way forward.

Finally, we focus on perhaps the most significant issue in practical terms, the *externalities* and displacement caused by sharing economy activity and pose questions as to *whether* regulatory intervention is necessary or appropriate in response.

3C: Intellectual Property (chair: James Griffin, BILETA Executive)
Edgar Graham Room (2nd floor)

Megan Rae Blakely	Lancaster University	Visually Mapping Intellectual Property and Human Rights

Our current global environment related to technological and artistic creation is regulated through intellectual property (IP) frameworks, providing limited exclusive rights in exchange for benefit of these works to the public. However, the 'limited times' continue to be extended, and beneficiaries continue to expand beyond the original author or inventor. The limited monopolies were designed to encourage and facilitate innovation and progress, but the balance appears to be tipping past facilitating human development to chilling such progress. Inevitably, laws related to these subjects will intersect with human rights on a practical level, such as the right to culture, education, and other social and economic rights. [1] However, the legal system has constructed disciplinary frontiers and borders. Traditionally, the human rights and IP fields have been studied, researched, and regarded as largely distinct areas of the law. Notable scholars have acknowledged the important, progressive overlaps and resulting impacts on these two fields although scholarship on the issue remains relatively sparse. [2] Whilst the distinctiveness remains, the language used in journals and legal instruments, over time, has begun to mutually incorporate the other's linguistics. [3] This convergence is only accelerating in light of technological advances facilitating social, culture, and creative connectivity.

Based on the concept of evaluating the use of discipline-specific language to uncover trends in legal and social practice, this article crosses boundaries amongst disciplines in substance as well as in methodology. It proceeds by setting out initial research on using natural language processing and other computer science methods to map the language used in the IP and human rights fields, in order to identify how the scholarship and legislation has progressively begun to incorporate the disciplinary language, which would indicate a shift in the legal and social perspective on IP regulation. The initial stages of this project are already underway in partnership with an undergraduate supervision of a computer science student at Bristol University, and further work is being undertaken with the computer science department at Lancaster University to use advanced permutations of natural language processing, data visualisation, and legal evolution.

In order to visually trace the development of international IP, laws will be charted on a three-dimensional chronological timeline, with an x-axis measuring the language and effect of the law toward human rights/access to IP/limited monopolies and a y-axis measuring creator/owner or user.

Discussion will include issues such as the false assumption that access itself encourages innovation and the appearance of a problematic and false dichotomy between human rights and IP and between user and creator that the charting system creates as well as solicit any scholarly advice on best practices for the ongoing development of the project. The outcomes of this mapping should not only contribute valuable insights into the historical development of IP law and the impact on human rights but also prompt consideration of the future impacts of IP law and technology uptake on cultural and social rights and practice.

[1] *See, e.g.,* Universal Declaration of Human Rights (1948); International Covenant on Economic, Social, and Cultural Rights (1966).
[2] Austin, G. and Helfer, L., eds, *Human Rights and Intellectual Property: Mapping the Global Interface*, (2011 Cambridge).
[3] Geiger, C., ed., *Research Handbook on Human Rights and Intellectual Property* (2016 Edward Elgar).

Abbe Brown	University of Aberdeen	Law below and beyond frontiers: marine genetic diversity, IP and information

The sea and life under it is important to all, in particular in Northern Ireland where 50% of its biodiversity is in the seas (Valuing Nature 2015). Scientific expertise can transform the oceans' raw materials - marine genetic resources (MGR) - into invaluable products (such as pharmaceuticals), to benefit society (Royal Society 2017). Further, 64% of the surface of the oceans is beyond the control of states. Accordingly, there are questions of which state or private entity should benefit from, and have responsibilities regarding, MGR and product development. Some key data demonstrates the scale and nature of these issues: 862 marine species have been identified; 12998 genetic sequences are associated with patents; and 47% of all patents including gene marine sequences are owned by BASF (Blasiak 2018).

In this context, a new international legally-binding instrument is being negotiated regarding MGR in areas beyond national jurisdiction under the United Nations Convention on Laws of the Sea (UNCLOS), building on General Assembly resolutions from 2004. Challenges include minimising obstacles to scientific research and commercialisation, including through regulatory obligations regarding access and benefit sharing; and avoiding overly enabling private control of MGR including through intellectual property rights and data, and any repeating of analogous challenges encountered in relation to public health and biotechnological and synthetic biology innovation (Correa 2017, Thamisetty 2018). A central point is whether MGR should be seen as free to all to take and own (the freedom of the high seas approach) or as being part of the common heritage of humankind.

This paper draws on interdisciplinary work between Law and Science (see https://www.abdn.ac.uk/ncs/departments/chemistry/bbnj/index.php), developing a new approach - a pragmatic solution (Broggiato et al 2018). This focuses on a notification and exclusivity period for researchers, and some sharing of data or samples. The proposal was shared with some success with diplomats, policymakers, lawyers, scientists and activists before and at the first UNCLOS IGC in 2018.

Developing a new regime in an unregulated space which raises questions of data and intellectual property, raises rich parallels with the internet regulation debate. A key distinction is of course the negotiation of a treaty. In this respect, internet and IP law can also provide important insights regarding intersections and fragmentation. Negotiations could involve IP, information, human rights, the law of the sea and access and benefit sharing in respect of biodiversity, and the

work of the Intergovernmental Oceanographic Commission - but to what extent would regard to this prevent the reaching of any outcome?

Substantive arguments, and strategic goals, will have been further developed in these respects by project team members for and at the second IGC in March/April 2019 (before the BILETA conference). This conference paper will share these experiences, and lessons gained, for future scholarship and policymaking when technology enables new frontiers to be explored and existing fields to clash in new ways - to minimise problems for the future.

Felipe Romero Moreno	University of Hertfordshire	'Upload filters' and human rights: when general monitoring obligations become a 'specific duty of care'

This paper critically assesses the compatibility of monitoring obligations with the right of users to a fair trial, privacy and freedom of expression under Articles 6, 8 and 10 of the European Convention on Human Rights (1950) (ECHR). The analysis draws on Article 15, Recital 47, Recital 48 of the E-Commerce Directive 2000/31/EC, Articles 13, 15, 16, 17, 82 of the General Data Protection Regulation 2016/679 (GDPR), as well as the case-law of the Strasbourg and Luxembourg Court. It considers the compliance of monitoring obligations with the European Court of Human Rights' (ECtHR) three-part, non-cumulative test, to determine whether these obligations can be adopted, firstly, 'in accordance with the law', secondly, pursuing one or more legitimate aims contained in Article 8(2) and 10(2) of the Convention and thirdly, be 'necessary' and 'proportionate'. The paper also examines the compatibility of monitoring obligations with the ECtHR principle of presumption of innocence under Article 6 of the ECHR. It argues that the implementation of such obligations may be compatible with the ECtHR's test and its principle of presumption of innocence. However, this would also require compliance with both, the E-Commerce Directive and the GDPR. Specifically, while 'upload filters' should not lead to general monitoring obligations being imposed on hosting service providers pursuant to Article 15 of the E-Commerce Directive, these so-called 'duties of care' should be 'specific' enough to observe Recitals 47 and 48 of the E-Commerce Directive, but also respect user GDPR rights. Namely, Article 13 (right to be informed), Article 15 (right of access), Article 16 (right to have inaccurate personal data rectified), Article 17 (right to erasure), and Article 82 (right to compensation). The paper proposes a new regulatory approach, which ensures that monitoring obligations can be implemented in a way, which is compliant with the Convention, the E-Commerce Directive 2000/31/EC and the GDPR. In particular, it suggests three key procedural safeguards: Firstly, accessible, transparent and auditable monitoring systems, which are less resource- intensive when it comes to data processing of users and their uploaded content and distinguish between non-personal data, personal data and sensitive data. Secondly, time- limited and specifically targeted user monitoring obligations aimed at particularly serious cases such as, commercial scale online copyright infringement. Lastly, streamlined complaints and redress mechanisms in which users have the right to have their affected personal data rectified and erased, as well as being able to claim compensation due to false positives that is, the blocking of lawful user-uploaded content and general monitoring being carried out on them.

3D: Data Protection (chair: Marek Martyniszyn, QUB)
Moot Court Room (2nd floor)

Maria Samantha Esposito	Politecnico di Torino	Human rights and technology development in the jurisprudence of data protection authorities

The current technological and social scenario, characterised by complex innovative solutions and data-intensive systems, raises new issues concerning data protection and suggests to place them in the broad context of human rights. This has recently induced legal scholars and policy makers to consider risk analysis and risk management models that go beyond the traditional focus on data quality and security.

The main challenge in the design of human rights-based assessment models concerns the outline of a general paradigm of values to be used as a benchmark in the assessment process. From this perspective, the main goal of this paper is to figure out whether and to which extent data protection authorities take into account human rights, both in their decisions and in the guidelines they provide.

In carrying out this analysis, the paper focuses on the approach adopted by the Irish and UK data protection authorities. Moreover, to provide a broader overview of the different approaches adopted at EU level, the opinions issued and the documents adopted by the Article 29 Data Protection Working Party and the European Data Protection Board are also considered.

From a methodological perspective, over 120 documents have been analysed, selected on the basis of their relevance with regard to human rights and fundamental freedoms. In this regard, the keywords used to extract the most relevant documents from the dataset of those adopted by the UK and Ireland data protection authorities took into account the nature of the devices used for data collection (e.g. video surveillance systems, IoT systems and personal devices), the contexts where data were collected (e.g. work context) or the nature of the collected data (e.g. biometric data).

Despite the different nature of the adopted documents, they show that a plurality of rights and freedoms – other than the right to privacy and the right to data protection – has been taken into account by these bodies. More specifically, these authorities consider the potential negative outcomes that may affect, for example, individual self-determination and autonomy, the freedom from discrimination, the personal identity, and the dignity of natural person.

Nevertheless, since data protection laws provide limited references to the protection of these interests, in several cases the importance of these issues emerges only indirectly from the observations made by data protection authorities. In particular, these authorities frequently use general data protection principles to safeguard interests other than those closely related to privacy and to the security of personal information.

The results of this analysis confirm the need to develop broad impact assessment models which consider the different human rights and fundamental freedoms likely to suffer prejudice in the context of intensive personal data processing operations.

Aysem Diker Vanberg	University of Greenwich	Data portability post GDPR: Does the right to data portability really work for social media platforms?

The General Data Protection Regulation [1] (the GDPR) came in to force on May 2018. Article 20 of the GDPR comprises a new right to data portability, enabling users to transfer their data to other electronic processing systems. Article 20 requires service providers to ensure that they can hand over the personal data they possess on a consumer in a usable transferable format. As an example this will allow a Facebook user to download their Facebook profile, photos, profile updates and other personal data and move it over to other competing social networking sites. Data portability is not only limited to social networking sites, it will be applicable to cloud computing, web services, smartphone systems and other automated data processing systems. As put forward by de Hert et al, the right to data portability is arguably one of the most important novelties within the GDPR, as it aims to empower individuals by giving them the right to control their data and the right is at the intersection between found at the intersection between data protection and other fields of law such as competition law, intellectual property and consumer protection [2]. However, it is unclear if the new right as articulated in the GDPR will be enough to support the development of genuine data portability, or if further measures will be needed to extend its scope and realise its full potential. There are also practical challenges associated with transferring data, the potential for weak incentives for the participation of companies who hold the data, and unclear 'ownership' rights regarding data, which has not been explicitly provided by the consumer.

In the light of the above, this paper will analyse the implementation of the right to data portability and whether it actually supports genuine data portability particularly in the context of social media platforms and e-mail providers. The paper will endeavor to incorporate an empirical study through creation of social media accounts with subsequent attempts to transfer data between different platforms to observe the practical implementation of this right and inherent difficulties surrounding it. Based on the research findings, recommendations will be made to realise the full potential of the right to data portability.

1 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance)
2 Paul de Hert, Vagelis Papakonstantinou, Gianclaudio Malgieri, Laurent Beslay, Ignacio Sanchez 'The right to data portability in the GDPR: Towards user-centric interoperability of digital services' Computer Law and Security Review (2018) 193.

Wenlong Li	University of Edinburgh	Beyond Individual Access to Personal Data: Making Personal Data Obtained through Making Data Portability Requests Useful for Data Subjects

A critical feature of the right to data portability that differs it from existing subject access mechanism is that this new right is not about seeking knowledge of data processing for further action, but devised to enable reuse of personal data at individual level. As the Article 29 Working Party (A29WP) notes, this was a missed opportunity that, in the Data Protection Directive, the right of access was prohibitively 'constrained by the format chosen by the data controller when providing the requested information'.

To some extent, the GDPR provisions, in together with the A29WP Guidelines, have removed these format constraints, allowing the new right to gain some values that are otherwise not present in the traditional right of access. The A29WP notes that this right 'supports user choice, control and empowerment' and in its view, this right has been even reframed as 'a right to reuse the (personal) data'.

That said, reliable reuse of data takes much more than getting a copy of data retrieved and transmitted. Beyond this, this paper first surveys what it takes, from a technical perspective, to render useful personal data obtained through making data portability requests in accordance with the GDPR. A layered, conceptual framework of personal data reuse is developed on the basis of data science literature, standardisation efforts (e.g. ISO/IEC) as well as the revised European Interoperability Framework. It is revealed that reuse of personal data depends upon several layers of technical specifications (transport, syntax and semantic) and the optimal method of achieving it varies from case to case (data archive, migration and analysis). Both GDPR provisions and A29WP Guidelines have, albeit in a less structured way, addressed several layers of data portability in order to ensure the usefulness of data in the hands of data subjects. A critical analysis of all these rules will indicate that the current framework has much to be improved.

The remaining part of the paper focuses on the role of (data protection) law in facilitating the optimal level of portability, and in particular, how the newly established European Data Protection Board may further carry on this task. It is noted that this new authority is faced with a dilemma between overextending GDPR provisions to ensure reuse of personal data, and reduce individual control over personal data to individual efforts to minimise data processing. To avoid both extremes, the A29WP Guidelines should be timely transformed into a more compressive, systematic and consistent framework, consisting of both general guiding principles and level-specific, purpose-oriented solutions.

4A: AI, Automation, and Algorithms (chair: Conor McCormick, QUB) Room 0G.009 (ground floor)		
Catherine Easton	Lancaster University	Autonomous Vehicles and disabled people: preliminary results from an on-going project

The trajectory of law and policy surrounding the implementation of driverless, or autonomous, cars has reached the point at which the UK has now passed specific technology-focused legislation such as the Automated and Electric Vehicles Act 2018. This links back to the UK Government's action plan to roll out this technology, in which it was stated that it has the potential to bring major benefits and change people's lives for the better. In this report, disabled people were identified as a specific group who could benefit from autonomous cars. The UK's legal and regulatory framework will need to adapt to implement this technology. However, it has been found that the experiences of disabled people are often overlooked in the development of law and policy relating to technology. This paper will outline the preliminary results of a project which aims to provide a critique of how the law relating to autonomous cars is developing, building in the perspective of disabled people from the outset. It has used qualitative methods to gain insights into attitudes towards safety, liability and privacy in relation to autonomous vehicles. These will be complemented with a co-design workshop in which policymakers, designers and disabled people will carry out exercises focusing on the interplay of law, regulation and technology design.

Alessandro Mantelero	Politecnico di Torino	Regulating data processing in the Age of AI

Predictive policing software, neighborhood aggregate credit scoring and many other algorithmic decision-support systems highlight how the potential negative outcomes of data use are no longer restricted to the widely recognized privacy-related risks. They also include other forms of prejudices (e.g. discrimination, restrictions on access to contents and digital services) that can be better addressed by placing data processing in the broader context of human rights and societal values.

The use of algorithms in modern data processing techniques as well as data-intensive technology trends suggest therefore the adoption of a broader view of data protection impact assessment. A view focused on the potential negative outcomes of data use on a variety of fundamental rights and freedoms, which also takes into account the ethical and social consequences of data processing. A recent evolution in this sense is evident in the initiatives adopted by the Council of Europe in the field of Big Data and Artificial Intelligence.

Against this background, the author points out how, over the years, the principles-based Convention 108 (and the recently adopted Convention108+) has become a cornerstone for a broader set of regulatory initiatives in the field of data protection, focused on several specific issues. This sectorial approach, which combines hard and soft law elements, provides a flexible manner to address the issues that characterise societies evolving under the pressure of technology development.

On the basis of this general analysis of the main challenges of AI and the possible regulatory approaches, this paper specifically considers the Guidelines on AI under discussion at Council of Europe level comparing them with the Declaration on Ethics and Data Protection in Artificial Intelligence adopted by the 40th International Conference of Data Protection and Privacy Commissioners, and with the Draft Ethics Guidelines on AI provided by the EU High-Level Expert Group on Artificial Intelligence.

In carrying out this analysis, this paper considers the role of the precautionary principle and the adoption of a human rights-oriented approach in addressing the potential outcomes of AI which affect both the individual and collective dimensions of data use. The risks of discrimination and extensive forms of data collection, as well as the adverse consequences of using de-contextualised data and de-contextualised algorithmic models will be further addressed. Finally, the paper points out the role that citizen engagement and participation can play in AI development and in the assessment of the impact of AI on human rights and societal values. This also in the light of the adoption of forms of algorithm vigilance focused on the prevention of the adverse consequences of AI applications.

Nynke Vellinga	University of Groningen	No frontiers for automated vehicles? The notion of 'driver' and international road traffic law

Automated driving is getting ever closer to reality, but legal developments are lagging behind. Technological boundaries are shifting each and every day, thereby stretching legal limits. The development of automated vehicles confronts lawyers with many legal questions across different legal fields. Questions are raised regarding the technical requirements for automated vehicles, liability for damage caused by automated vehicles and questions concerning the protection of the data gathered by the automated vehicle. This contribution, however, will focus on the legal questions automated driving raises for international road traffic law. The answers to these questions are of great importance as automated vehicles cannot drive down public roads without there being clarity on these issues. Cross-border traffic has been made possible by two international road traffic conventions: the Geneva Convention of 1949 and the Vienna Convention of 1968. These Conventions are of global importance: over 90 countries are party to the Geneva Convention, over 70 countries are party to the Vienna Convention (some of which are also party to the Geneva Convention). The national traffic laws of these countries need to be in conformity with the Convention the country is party to. Both Conventions enable easy cross-border traffic by determining, among others, traffic rules. This is why, when crossing for instance the border between Northern Ireland and Ireland, many traffic rules stay the same. The notion of 'driver' is omnipresent in these traffic rules of both Conventions. The Geneva Convention and the Vienna Convention are both based on the notion that every moving vehicle has a driver. The purpose of automated vehicles, however, is to increase road safety by taking the human driver out of the loop. Therefore, automated driving poses challenges for the Geneva Convention and the Vienna Convention. This contribution will show that an automated vehicle does not have a 'driver' within the meaning of the Conventions. The automated vehicle is, within the meaning of the Conventions, truly driverless. The Conventions will therefore need to be

revised in order to accommodate automated driving. There are several ways in which the Geneva Convention and the Vienna Convention can be changed so as to accommodate automated driving. Examples from international aviation traffic law and Dutch criminal law will be used to come to different approaches of revising the Conventions. The different approaches will be compared in order to identify their (dis)advantages and their feasibility. All these approaches could lead to revised Conventions or, more drastic, a new convention on road traffic, that accommodate automated driving, so that in the future cross-border traffic will not be impaired by the absence of a human behind the wheel.

4B: Regulation (New Approaches) (chair: Paul Maharg, BILETA Executive)
Stephen Livingstone Room (2nd floor)

James Griffin	University of Exeter	The changing nature of digital law

We might argue that law is becoming more digital in nature - but what does this mean? Often when we refer to law regulating digital technologies, we are referring to analogue laws. For example, the US Digital Millennium Copyright Act 1998 favoured the use of certain digital technologies to prevent unauthorised access and reproduction of digital works - but the Act was not digital itself. This is true even of actions for blocking injunctions, say under the UK s.97A CDPA 1988, as although they direct the technology very precisely, they do not directly interface with the ISP system. Pure digital law, on the other hand, could involve law that is already in digital format. It could be self-executing if applied. There is a precursor of such a system with the quango UK Copyright Hub, an attempt to place legally enforceable licensing standards within an official set of digital, programmable, rules. Where all parties have a combined interest in using such a system, for example in resolving disputes, then there is clear potential for such a system becoming popular, even commonplace. Digital platforms have already been used in certain specific areas, e.g. family and property.

The characteristics of digital technology are key, and more so the 'digital' than the 'technological'. We should not forget the wide meaning of 'technology' – analogue laws themselves could be considered a technology (per Heidegger), so it is primarily the utilisation of those laws in the digital context that is important. With the rise of the "information society", digitisation is covering more types of work. Today, even DNA could be considered 'digital' due to its ability to store digital data. That which is digital is also more likely to be editable. Law could become immediately enforced, able to change according to the code presented to it. Digital law could be self-executing; it could also involve artificial intelligence. This paper considers the changes that could result, and the consequences of that upon those governed by the law. The paper also suggests some initial steps in dealing with some of those consequences.

Edina Harbinja Vasileios Karagiannopoulos	Aston University University of Portsmouth	Web 3.0 (4.0) or DWeb – the decentralisation of the internet?

Web 3.0 is, arguably, the next step in the development of WWW technology. It is a 'semantic web', which can process, combine and interpret information better to provide users with a more enhanced, interactive experience. The next step, looking further into the future, would be Web 4.0 or 'social machines' [1], an immersive and super intelligent web, based on powerful machine learning and AI technologies and applications. The above developments are driven by very powerful IT conglomerates ("the GAFA" - Google, Apple, Facebook, and Amazon) and one has to wonder whether there could be an alternative paradigm. Here is where the development of the DWeb comes to offer an alternative to our future web reality.

The DWeb promises to decentralise user experience and challenge the current dominance by corporate platforms as well as offer more competition and enhanced privacy. It is not based on the location of the user and single servers using HTTP protocols (IP address), but on protocols that identify content and enable information sharing on a peer-to-peer basis. This benefit could be further reinforced by challenging the information control currently established by large internet corporations, rather than users, which in turn could enhance user privacy. However, the Dweb also poses challenges for policing criminal activity online and generally imposing any kind of regulation, as with every decentralisation-focused structure, which does not make it appealing to the status quo.

Dweb is still at its very early stages, but its rationale is consistent with the cyber-libertarian hopes of the past [2] in terms self-regulation and decentralisation of control. It also reinforces the idea that users are not merely passive and can still organise and influence the regulatory interplay between governments, legislators and big corporations in order to shape their Web experience. However, realising such an enormous paradigm shift would require a radical rethinking of our socio-political structures and the big question is whether the DWeb can be a driver for such a change in our information-based societies.

In our paper, we argue that the premise of the Dweb as an alternative in a capitalist market society is seriously challenged because conceptually our current socio-economic structures are geared towards profit based *en mass* and multifaceted exploitation of information. Consequently, the debate about the viability of the DWeb boils down to convincing users to move towards an alternative, more dynamic and responsibilised information-generating and sharing future.
We, therefore, explore whether the success of the Dweb relies on it becoming the stepping stone for reinventing our information-based economic and regulatory models. We will discuss whether the Dweb could be construed as a modern structure of reclaiming control of information production, knowledge and power by users. We attempt to evaluate its potential using regulatory and political theories around the topics of technology, control and dominance as we assess its viability and future regulability.

[1] Jim Hendler and Tim Berners-Lee, 'From the Semantic Web to social machines: A research challenge for AI on the World Wide Web' *Artificial Intelligence*, Volume 174, Issue 2, February 2010, 156-161.
[2] John Perry Barlow, *A Declaration of the Independence of Cyberspace*, https://www.eff.org/cyberspace-independence

Carl Vander Maelen	Ghent University	The impact of alternative regulatory instruments (ARIs) on globally operating tech companies: fragmentation or harmonisation?

The services offered by tech companies such as Google, Amazon and Apple have become inseparable from modern life. However, the stark reality that the ICT sector is a global, fast-evolving and complex industry has caused regulators across the world significant concerns. They face jurisdictional issues, varying levels data subject protections across countries and continents, and enforcement issues.

Against this background, more and more regulators are becoming conscious of the limits of traditional legislative instruments, and instead turn to alternative regulatory instruments (ARIs) such as codes of conduct and co-regulatory instruments (European Parliament, Council and Commission, 2016). Increasingly, their use is explicitly integrated in legislative instruments to allow for participation by stakeholders to implement public policy objectives. This is also the case for the EU's new data protection framework: the General Data Protection Regulation (GDPR). Its articles 40 and 41 GDPR encourage the drawing up of codes of conduct, which are soft law mechanisms that "rely on decentralizing regulatory authority among public, private and public-private actors and institutions" (Hagemann et al., 2018). According to the GDPR itself, they can help "calibrate the obligations of controllers and processors" (recital 98) and "contribute to the [GDPR's] proper application" (article 40). The European legislator thus clearly considers codes important tools to implement the GDPR.

The legal issue at hand concerns the role of ARIs in the regulation of global private actors that operate in jurisdictions across the world, particularly regarding data protection. Some claim the GDPR might lead to a **fragmentation** of the worldwide web by creating a 'European firewall' of strict rules (Floridi, 2014), whereas others maintain that the stringent norms might lead to a **harmonisation** of higher data processing standards around the globe. It is the hypothesis of this research that **articles 40 and 41 GDPR, in turn, amplify either possibility because of their unique role in furthering the implementation of the GDPR.** For example, it could be hypothesised that if Google binds itself to a GDPR-based code of conduct, the company might harmonise its data processing standards outside the EU with these GDPR standards since it might be economically advantageous (or better fits with its Corporate Social Responsibility strategy) to pursue a uniform data processing policy, regardless of jurisdictions. Alternatively, Google might only comply with the GDPR for its EU operations and maintain less strict data processing strategies in other jurisdictions, thus exacerbating GDPR-induced fragmentation.

This intriguing prospect of potential extraterritorial effects by non-legislative tools takes place on two levels: the micro-level (i.e. practices by global actors that are bound by the codes in a certain jurisdiction) and the macro-level (policy-making and standard-setting outside of the jurisdiction that they are adopted in). As a result, the implementation of ARIs could hugely impact the debates concerning the regulation of global private actors, on the one hand, and the calls for international data protection standards, on the other hand.

European Parliament, Council of the European Union and Commission of the European Communities, "Interinstitutional agreement on better law-making" (13 April 2016).

Floridi, L., 'Google ethics adviser: The law needs bold ideas to address the digital age', *The Guardian* (4 June 2014) https://www.theguardian.com/technology/2014/jun/04/google-ethics-law-right-to-be-forgotten-luciano-floridi.

Hagemann, R., Skees, J., and Thierer, A., "Soft Law for Hard Problems: The Governance of Emerging Technologies in an Uncertain Future", *Colorado Technology Law Journal (forthcoming)*, February 2018, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3118539.

4C: Intellectual Property (chair: Felipe Romero Moreno, BILETA Executive)
Edgar Graham Room (2nd floor)

Ruth Flaherty	University of East Anglia	"Culture? Where we're going we don't need culture!" An empirical investigation into the importance of unauthorised derivative works to society in the digital age and how Article 13 undervalues them

Could anyone other than Doc Brown have driven the DeLorean DMC-12 to 88mph, the future, and fame? Would Westeros be fundamentally different if Viserys married Khal Drogo, 'crowned' Daenerys, and walked into fire with the dragon eggs? Questions like these are asked by fans of the work on fanfiction archives such as Fanfiction.Net. As early adopters of many forms of social media – such as forums, blogs and online archives – the fandom group provides a fascinating case study of the effect of unauthorised derivative works on the consumption of media products. Most existing literature on the subject has been ethnographic in nature and focused on the literary and media implications of fan activities. While legal research exists, most is doctrinal and based within the US legal system. This paper adopts a distinctive approach, applying quantitative methods to test the economic biases within copyright law as they apply to unauthorised derivative works of this type. This will demonstrate that fan fiction should be protected within the as-yet undefined 'pastiche' fair dealing copyright exception within S30A CDPA 1988. By using a dataset of user posts from the world's largest online fanfiction archive (Fanfiction.Net) and sales data (Nielsen), this study further suggests that Article 13 of the Proposed Directive on Copyright in the Digital Single Market contains serious misapprehensions regarding culture in the digital age. Application as it stands may harm culture more than it protects it. This research suggests that existing theories of copyright harm are incomplete, and that there may be important social incentives and welfare benefits to permitting this type of use. These are not taken into account by standard copyright and economics theory that presumes fans to be interfering with the 'normal exploitation' of the underlying work and thus harming the 'legitimate interests' of the rightsholder. This research is important as it uses data to draw together and test previous research into copyright law and media production and consumption, thereby enabling conclusions to be drawn regarding how the diverse interests of authors, publishers, readers and society as a whole should be balanced in the digital age.

Pradeepan Sarma	Vrije Universiteit Brussel	The 'Integrity' of Canada's 'Users' Rights Doctrine'? A Dworkinian Approach

In 2004, the Supreme Court of Canada created the doctrine of "user rights" in Canadian copyright law, which introduced into Canadian jurisprudence the idea that Canadian copyright law represents a balance between "creators" and "users", creating a new framework for what had previously been narrowly interpreted exceptions to copyright infringement. Having been associated with the fair dealing doctrine since its introduction into Canadian law, in 2012 another users' right was identified: the retransmission of broadcast television by broadcast distribution undertakings. The vastly different nature of this exception as compared to fair dealing required past explanations and justifications for users' rights, so intertwined were they with the fair dealing doctrine, to be revised and re-evaluated.

A comprehensive account of the users' rights doctrine in Canadian copyright law has yet to be made. In this paper I analyse the nature of the "users' right" using Wesley Hohfield's schema of juridical relations and evaluate the users' rights doctrine through Dworkin's interpretive theory of law to find the principle that best fits and justifies the doctrine. My paper suggests that the dissemination of work acts as a coherent guiding principle behind the users' rights doctrine, distinguishing it from the treatment of 'users' in other jurisdictions and allowing for uses that perhaps better reflects a conception of creativity and cultural consumption that is well-suited both to the actual process of repurposing and cross-fertilization that defines creative practice and to our current networked information societies where the spaces through which we engage the world are usually not part of the public domain as envisioned in copyright theory but increasingly proprietized. On the other hand, the inclusion of non-creative uses into this doctrine allows it to be captured by 'users' that were not necessarily intended, such as corporate actors.

Amy Thomas	University of Glasgow	EULAs in eSports and video game streaming: copyright as a new commercial imperative for game owners

At the inception of eSports in the 2000's, its stratospheric growth could not be anticipated; what was then a niche subculture has since morphed into a global industry worth millions. Predominantly grounded in youth and internet sharing culture, streaming gameplay both in solo-play and tournaments has been fundamental to growing eSports' popularity. Now, those streams have commercial value that is not just limited to the mutual benefits that may be brought by users acting as a means of indirect marketing. Questions concerning broadcasting rights and copyright in gameplay have become a commercial imperative; should game owners adopt business models which err towards exclusivity (and ergo giving those rights more value), or maintain a relatively open sharing ecosystem in line with its origins?

The fact that this exclusivity is an option at all has been raised as a concern at the first EU Parliamentary discussion on eSports. Unlike traditional sports, which have no underlying copyright protection in the sport itself as such, eSports players are dependent on a commercially-owned product. Game owners therefore have the capacity to become sole arbiters of access in what in principle should be an unpredictable game of contest; this, speakers opined, has the capacity to result in monopoly. Regardless, eSports has been left (for the moment) to self-regulate.

One of these self-regulatory mechanisms is the end user licensing agreement (EULA), the main tool for regulating gameplay broadcast both in the amateur and professional context. We see that the strategic use of this particular manifestation of copyright in fact disguises a larger question on the boundaries of executive ownership within the video game industry; how defensible is such an exclusive top-down power structure in what increasingly resembles a "real" sport? In particular, this may cause issues for intermediaries such as tournament hosts, who may be in exclusive deals with game owners to broadcast this content. Despite these agreements, tournament hosts have been criticised for

attempts to remove any user-uploaded content which encroaches said exclusivity (Azubu/SpectateFaker, Electronic Sports League/Dota 2). Questions of intermediary liability in the necessarily international context of eSports are only likely to become more complicated amidst recent policy developments (namely article 13 of the Copyright in the Digital Single Market Directive, combined with Brexit).

These questions live and die by the EULA. As such, this discussion will explore examples of these agreements and where they fall on the open-exclusivity binary. Anecdotal evidence will also be explored on how game owners and users navigate EULAs in practice, and how this is related to broader questions of intermediary liability.

4D: Data Protection (chair: Karen Mc Cullagh, BILETA Executive)
Moot Court Room (2nd floor)

Mark Leiser Bart Custers	Leiden University	The Law Enforcement Directive's Consent and Categorization Quagmire

Passed in synchronicity with the General Data Protection Regulation (GDPR), the Law Enforcement Directive (LED) has been heralded for its role in building "an area of freedom, security and justice with a high level of data protection, in accordance with the EU Charter of Fundamental Rights". Data processed for 'law enforcement purposes' by 'competent authorities' must comply with principles of necessity, proportionality & legality, while ensuring appropriate safeguards in place for data subjects. Despite an increase in scope, applicability, and rights and freedoms of individuals, there is ambiguity as to how the LED should work in practice. This is due to both conceptual and practical issues that the LED raises. From a conceptual perspective, three issues are discussed. The first issue concerns the role of consent in the LED. Although the LED uses consent as a central concept, this is fundamentally at odds with the processing of personal data in a law enforcement context. The second issue is that the LED requires competent authorities to categorize data relating to witnesses, suspects, and victims. This is problematic, because a participant's role in a criminal event is both fluid and dynamic and the roles of data subjects typically change over time or sometimes even overlap. The third issue is that the LED requires competent authorities to document whether data collected is a 'fact' or an 'opinion'. The problem here is that 'factual' accounts of witnesses and others are always inherently subjective. The LED´s requirement on competent authorities to categorize facts from opinions and for controllers to make a clear distinction between offenders, suspects, witnesses, and victims puts recognized data protection principles of lawfulness, fairness, transparency in the crosshairs. From a practical perspective, the national implementation in EU member states raises issues. This is illustrated by examining the UK and Dutch approaches to the concept of consent, a fundamental and controversial aspect of data protection law. It is concluded that, while in some respects the LED brings data controller obligations for law enforcement authorities into the 21st Century, the LED contains conceptual issues and, in comparison to the GDPR, contains limited transparency requirements, lower thresholds for consent, and, in some areas, lower standards for protecting data subject rights. Although the LED requires EU Member States to establish appropriate time limits for the erasure of personal data, a careful balance of rights is required to ensure a victim's opportunity for justice is not 'deleted'.

Ingrida Milkaite Eva Lievens	Ghent University	Consent, contract and legitimate interests as grounds for lawful processing of children's personal data in the EU: investigating an unexpected turn of events

Children that grow up today do so in a digital environment in which through a variety of devices and services personal data is processed in unprecedented quantities (Lievens, Livingstone, McLaughlin, O'Neill & Verdoodt, 2018). The European Union's General Data Protection Regulation (GDPR) acknowledges that children's personal data merits specific protection (recital 38).

The GDPR provides for six specific grounds which can be used to lawfully process personal data of (child) data subjects. In short, these are consent, contract, legal obligation, vital interests, public interest and legitimate interests (article 6 GDPR). Initially, in the run-up to the implementation of the GDPR and just afterwards, both in scholarly and public discourse, the major focus was on consent which people were required to provide (anew) (Macenaite & Kosta, 2017; Milkaite, Verdoodt, Martens & Lievens, 2017; van der Hof, 2017; Borgesius & Lievens, 2018; Milkaite & Lievens, 2018). In practice, however, other grounds for data processing are being used more widely than previously foreseen. Facebook, which also owns Instagram, claims to rely on all six grounds (Facebook, 2019), Google relies on consent, legitimate interests, contract and legal obligations (Google, 2019). Two other services, extremely popular among children and teenagers – Snapchat and TikTok – rely on contracts, legitimate interests and consent (with Snapchat but not TikTok also including legal obligations) (Snap Inc., 2019; TikTok, 2019).

These findings raise legal questions that were not fully anticipated, especially in relation to children. The rather heavy reliance on legitimate interests, for instance, puts into question how the exemption foreseen in article 6 (1) f) GDPR ("*except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child*") should be interpreted. How the particular requirements that are connected to each legal ground are or should be balanced with *children's* rights, interests and their specific needs will be the central research question of the proposed paper.

This analysis will be carried out through, first, a detailed mapping of the privacy policies of Facebook, Google, Snapchat and TikTok, and, second, an investigation of the opinions and guidelines provided by the Article 29 Working Party and European Data Protection Board, recent academic doctrine, interpretations provided by the national data protection authorities. A specific focus will be on the practices of the Irish Data Protection Commission which is of particular importance in this context as many EU subsidiaries of global ICT companies, such as Facebook and Google, are based in Ireland.

Borgesius, F. Z. & Lievens, E. (2018). Commentary Article 8 GDPR, Conditions applicable to child's consent in relation to information society services (forthcoming). In *GDPR Commentary*. Edward Elgar Publishing.
Facebook. (2019, January). Data Policy (What is our legal basis for processing data?). Retrieved 11 January 2019, from https://www.facebook.com/privacy/explanation
Google. (2019, January). Privacy Policy. Privacy & Terms (European requirements). Retrieved 11 January 2019, from https://policies.google.com/privacy?hl=en&gl=be
Lievens, E., Livingstone, S., McLaughlin, S., O'Neill, B. & Verdoodt, V. (2018). Children's rights and digital technologies. Retrieved from https://lirias.kuleuven.be/handle/123456789/596812
Macenaite, M. & Kosta, E. (2017). Consent for processing children's personal data in the EU: following in US footsteps? *Information & Communications Technology Law*, *26*(2), 146–197. https://doi.org/10.1080/13600834.2017.1321096
Milkaite, I. & Lievens, E. (2018, June 28). GDPR: updated state of play of the age of consent across the EU, June 2018. Retrieved 11 July 2018, from https://www.betterinternetforkids.eu/web/portal/practice/awareness/detail?articleId=3017751
Milkaite, I., Verdoodt, V., Martens, H. & Lievens, E. (2017). *The General Data Protection Regulation and children's rights: questions and answers for legislators, DPAs, industry, education, stakeholders and civil society. Roundtable Report.* Retrieved from https://www.betterinternetforkids.eu/documents/167024/2013511/GDPRRoundtable_June2017_FullReport.pdf
Snap Inc. (2019, January). Privacy Center (Users in the European Union). Retrieved 11 January 2019, from https://www.snap.com/en-US/privacy/privacy-policy
TikTok. (2019, January). Privacy Policy (How we use your personal data). Retrieved 11 January 2019, from https://www.tiktok.com/
van der Hof, S. (2017). I Agree. . . Or Do I? — A Rights-Based Analysis of The Law on Children's Consent in the Digital World. *Wisconsin International Law Journal*, *34*(2), 101–136.

Paul Quinn
Gianclaudio Malgieri
Vrije Universiteit Brussel

The Concept of Sensitive Data – Still fit for purpose?

Data protection frameworks are becoming ever more prominent (and even dominant) in terms of legal approaches that are intended to foster personal privacy. This is exemplified by the breadth and reach of the EU's General Data Protection Regulation (GDPR). The concept of sensitive (or special data) has long been central to data protection frameworks. It relates to types of data for which the processing of which entails a higher regulatory burden. This is because the processing of such data is considered to bring with it greater risks in terms of both individual privacy and risks for society. Consent for the processing of such data has for example traditionally required more formality. This may have entailed the need for physical consent forms or other related measures. In recent time the nature and use of sensitive data has been changing at a rapid pace. Increases in computing power, the availability of ever more powerful algorithms and the ability to combine disparate sources of data means that the volume of sensitive data is increasing at an almost exceptional date. In addition, the increasing acceptance and utilisation of various forms of electronic and online consent have begun to displace more traditional forms of formal consent for sensitive data. These changes raise questions as to the continued value of the concept. Is it still fit for purpose? Is the concept subject to a form of 'inflation' that will ultimately devalue it? This presentation will, largely using the example of health data, address these issues. This will include new requirements introduced by the GDPR relating to sensitive data. It will show that whilst the value of explicit consent may not (in the modern digitised age) be what it once was, other new procedural requirements incumbent on controllers of personal data mean that the concept still has considerable significance. Given that the scope of sensitive data is ever increasing these requirements will apply in ever more contexts and thus create further burdens for for those who wish to process sensitive data.