5A: AI, Automation, and Algorithms (chair: Mary Dobbs, QUB)
Room 01/004 (1st floor)

Adam Harkens	Queen's University Belfast	Frontiers of decision making: Algorithmic profiling, subjectivity and the legal environment

This paper explores the effects which algorithmic decision making technologies produce for legal subjects, by embracing the conference theme and conceiving of the legal environment as a set of frontiers comprised of competing regulations, designs, standards, ethics and procedures. Increasingly, digital technologies and algorithms are being incorporated into this environment to meet the needs of institutional innovation. Scrutiny around these processes has progressively grown in recent times. This is demonstrated by, among others, developments such as the Law Society of England and Wales' launch of the *Technology and the Law Policy Commission*.

Much initial research on algorithmic decision making in the law focused on the area of criminal justice. For example, on COMPAS in the United States - a web-based 'fourth generation' risk and needs assessment instrument – and Durham Constabulary's HART, the first example of an operational algorithmic risk assessment tool in the UK. However recent developments have shed light on the traction that these methods are gaining in a number of other areas of government in the UK, including most notably welfare and immigration. Data sharing processes are also on the rise across the EU, and this will remain the case following Brexit, by virtue of the Data Protection Act 2018. This ongoing process will produce challenges for lawyers and legal researchers alike, as they will need to understand changes in the protections and procedures afforded to legal subjects, how individuals are judged, and how these transformations are interlinked. The question remains as to how this should be addressed, researched, and potentially challenged.

The paper proposes that a broad view of legal systems and the function of law, conceived of as the legal environment, is required in order to understand the transformations currently taking place, and the potential options that are open in order to direct these. It does so by tracking developments in the use of algorithmic decision making and profiling technologies - elaborating upon the conflicts between regulation, policy, values, and the materiality of algorithmic tools, which contribute towards the 'frontiers' we are faced with - and arguing for a greater focus on the latter in terms of how legal subjectivity is affected. It concludes by discussing how to direct future research through this lens.

Marion Oswald	University of Winchester	Back to 'lie detectors' of the past to suggest ways of dealing with a machine learning future

The first part of the twentieth century witnessed considerable enthusiasm in the United States for the potential utility of the polygraph, or 'lie detector'. Its use in criminal cases was supposed to mark 'a new era, free from the crude third degree methods' (Floch, 1949-50). Claims were made for high degrees of certainty, even that polygraph methods were 100% efficient and accurate (Goldberg, 1949). Yet the claims of magic infallibility for the lie detector were contested from the start. Even one of the inventors of the modern polygraph, Leonarde Keeler, argued that there was no such thing as a 'lie detector' (Keeler, 1934).

The lie detector has been described as a modern version of the medieval 'ordeal' (Underwood, 1995). Present-day machine learning can suffer from similar magical thinking (Hildebrandt, 2018; Naughton, 2018), with Google's Ali Rahimi recently describing machine learning as 'alchemy' (Science, 2018). The polygraph machine cannot 'detect lies'; it merely records bodily changes, and human interpretation of its results is required for any diagnosis of deception. Neither can a machine learning tool independently 'predict' risk or a person's future; rather real world experience is reduced to variables (Hildebrandt, 2018) and an algorithm trained to detect patterns or similarities based on probabilities. The interpretation of the output as a prediction is a human one.

This paper will look back to mid twentieth century case-law and journal commentary that considered whether polygraphs had a place in the criminal law investigative and trial process, and in the vetting of staff. It will highlight a number of rules and proposed principles and standards that emerged, including from the interweaving of technology with human decision-making, and how these could help guide the integration of machine learning into present and future decision-making. The early arguments played out in court over the use of the polygraph might suggest a wider struggle between utilitarianism and justice as fairness, arguably something that continues today in the debates over the deployment of machine learning within high stakes decision-making environments. Finally, even if a 'perfect' machine learning tool was created that could be substituted for a human decision- maker, does comparison with the polygraph experience suggest that such a tool is likely to be accepted by society as a final arbiter?

Jan Zibner	Masaryk University	Subjects' Relevance within an AI-included Creative Process

There is an indisputable role of human interactors when speaking of the works created by or using artificial intelligence (AI) either in form of specialized software (as the portrait of *Edmond Belamy* or project *Next Rembrandt*) or an interactive platform (as the *DeepArt's* or *Humtap's* outcomes). Within such an AI-included creative process, we can find a lot of subjects interacting with an AI, either as (i) the authors of an AI per se, (ii) the authors of all the datasets used for creating a basic framework, which serves as an environment for creating the final works, or (iii) the users of an AI providing input data for it to create the works. All these subjects have potential IP rights to the resulting works, even if there is no strict answer to who are the real authors of the final works. Considering the principle of objective authorship in most of the law orders and the regimes of computer-generated works operating with undertaking the arrangements necessary for the creation of the work, it is needed to answer the question of uncertain authorship and its possible allocation.

Based on that, the paper analyses the question of how relevant the contribution of above-mentioned subjects is for the creative process and for the final work per se, and what could be their potential authorship claim. The problematics are analysed in the general theoretical way reflecting possible national aspects of law systems applying the principle of objective authorship (within the EU and focused especially on the Czech and British legal systems). For this purpose, the theoretical model will be specifically made up reflecting the existing models, their specifics and plurality of the participating subjects. This way ascertained conclusions can be used for the proper setting of the copyright scheme in the question of works created by or using an AI.

5B: Regulation (chair: Abhilash Nair, BILETA Executive)
Stephen Livingstone Room (2nd floor)

Mark Leiser Alan M. Sears J. Pieter Kalis	Leiden University	Zero-rating in Net Neutrality: when does it "materially reduce consumer choice"?

A data-free, or "zero-rated", music service was at the heart of a recent legal action involving T-Mobile, the Dutch consumer protection regulator, and a digital rights advocacy group. The latter brought an action in the Dutch courts to get the regulator to enforce an outright ban on the practice of packet discrimination passed into Dutch law in 2012. The Court ruled that T-Mobile's introduction of a music service from certain contracted providers was permitted under Article 3 of the European Union's Net Neutrality Regulation.[1] On appeal, the Court undertook a thorough review of T-Mobile's 'Datavrije Muziek' service, finding that the contractual requirements affirmed the non-discriminatory character of the service and did not limit end-user rights. Bits of Freedom, the Dutch NGO that sought the enforcement order, argued that data-free music streaming services obfuscated the market and undermined innovation. The concept of 'positive net neutrality' violations sits in stark contrast to 'negative neutrality' violations. The latter is normally associated with the blocking and throttling of content that threatens an Internet Service Provider's (ISP) business model. However, T-Mobile's zero-rated music service is an example of treating some content more positively than general Internet traffic. With the European Commission set for a public consultation on zero-rating, and The Body of European Regulators for Electronic Communications (BEREC) set to issue guidelines on the practice, the paper assesses the present state of positive net neutrality violations around Europe, focusing on differentiation cases to assess what types of positive net neutrality violations could result in a "material reduction on consumer choice". As zero-rating is limited to subscriptions that include a data cap, the Office of Economic Development has warned regulators to be vigilant against practices that could result in users constantly monitoring their data usage or limiting access to non-zero-rated services. The practice of 'zero-rating' poses a unique challenge to regulatory authorities keen to protect net neutrality. While consumers perceive free access to certain services as providing a benefit, zero-rating can also contravene the general aims of the Regulation: that Internet traffic is managed by internet service providers in a non-discriminatory manner and that consumer choice is protected. However, while the practice may be seen as beneficial to consumers, zero-rating can also affect the number of providers entering the market and compromise the "guarantee the continued functioning of the internet ecosystem as an engine of innovation".

David Mangan	Maynooth University	Common law meets cyberlaw: Canadian privacy and defamation in comparative context

Exploring the overlap and distinction between defamation and privacy constitutes a hurdle in the development of the law's engagement with reputation issues. This discussion focuses upon Canada. It is envisioned that the tort of defamation will be limited as a means of redress. Where the remarks made fall outside of the parameters of defamation, there will be a search for other tools the law may provide. To this end, claims in breach of confidence (in Canada this has been treated as a hybrid of tort and equity) and invasion of privacy are canvassed.

An action based upon privacy will be used where information is disclosed (i.e. published or passed on to others in some form) that may 'harm' reputation. The likely claim is that the information was obtained or released through some breach of privacy or confidence. The alleged contravention may be defined as either physical or informational (though there is overlap). Breach of physical privacy would arise where there is a breach of physical space wherein there was an expectation of privacy. Breach of informational privacy focuses on disclosure of information intended to be kept private. Here, information gained through confidence or information lawfully collected but misused in some way would be examples. There is overlap amongst these areas. Breach of physical privacy may also entail breach of informational privacy. Breach of confidence can arise when information obtained in confidence is disclosed.

Noting the influence of American jurisprudence on Canada in the area, a useful frame of reference here will be the law in the U.K. and E.U. (particularly decisions of the European Court of Human Rights) because there has been a pronounced engagement with defamation and the protection of privacy through the interpretation of the *European Convention of Human Rights* (ECHR) (articles 8 (privacy) and 10 (freedom of speech)). The touchstone for these discussions remains their implications for the law of defamation and privacy in Canada in an era that stretches the boundaries of this tort from its origins in print media.

Mehmet Unver	Anglia Ruskin University	What response to be given to the 'automated society' phenomenon? Discussion over the EU regulations on digital platforms

Artificial intelligence (AI), intruded into our society with the techniques used to enable profiling and predictive analysis, end up automated decision-making processes. Albeit with the variety and degrees, enhancing techniques and exponential growth of AI point to a prospect increasingly woven by cognitive and manipulative technologies (including natural language processing, machine learning, deep learning), which bear undeniable challenges. Albeit with a great many benefits (e.g. diagnosis of diseases, fraud detection in financial services), AI and accompanying technologies largely phase out human intelligence, potentially leading to an 'automated society'.

At the centre of this phenomenon lies the digital platforms (i.e. Google, Facebook) that extensively rely on AI-inclusive techniques (in personalized prices, recommendations, experiments, etc.) and are of a massive potential to transform the society. In the future, using sophisticated manipulation technologies, these platforms will be able to steer us through entire courses of action, be it for the execution of complex work processes or to generate free content for Internet

platforms, which signifies a trend from programming computers to programming people. [1] Remarkably, over-dependence onto the digital platforms means a material exposure (to the automated decision-making processes and their influences) which needs to be examined in terms of the regulatory response they receive vis-à-vis the societal impact they pose.
European response to digital platforms has so far become a semi-traditional (hybrid) approach by which both regulatory and self-regulatory actions are envisaged to end up transparent and non-discriminatory platform services. EU's regulatory response appears at several levels, i.e. from transparency of platform-to-business (P2B) relationships to data access and portability. The responsive safeguards reflect on the concerns surrounding Digital Single Market (DSM) often echoed with the uninterrupted cross-border flow of data along with transparency and information obligations on the so-called online intermediaries (digital platforms). Notwithstanding, 'automated society' phenomenon emerging out of the (data and AI driven) platforms seems to be obscured behind the background concerns and responsive tools.

While the EU regulations aim at protecting the users (both consumers and businesses) *individually* by means of the transparency, portability and information obligations, the resultant (cumulative) effect would hardly turn out to be a *collective* response on the part of the users. Individual protection of the users does not effectively result in the resilience (awareness and dignity) needed against the exponential and massive growth of AI that potentially leads to the 'automated society'.

Against this challenge stemming from the digital platforms and the underlying (AI) technologies, societal and collective intelligence should be in place. While a fully-fledged regulatory design exceeds the scope of this study, it is examined how such a collective response could be achieved, going beyond the individual solutions to be derived from the EU package. It is concluded and recommended that the starting point be setting out the guiding principles and values (including inclusiveness, participation, empathy, responsible innovation, decentralisation) that would pave the way to reconstruction of the 'collective intelligence'. It is also suggested that these principles be not value-free and just protective, but mitigative and transformative against the strong signals towards the 'automated society' phenomenon.

1. Dirk Helbing et al, 'Will Democracy Survive Big Data and Artificial Intelligence?' in D. Helbing (eds), Towards Digital Enlightenment: Essays on the Dark and Light Sides of the Digital Revolution, (Springer, 2019), 75-76.

5C: Copyright (chair: James Griffin, BILETA Executive)
Moot Court Room (2nd floor)

Sweta Lakhani Sanjeev Sahni	O.P. Jindal Global University	Fighting Plagiarism: Intellectual Property Rights Violations in Education in India

In recent times, the internet has allowed students, authors and academicians across the globe to access information easily and with few boundaries. Such instant availability and accessibility of the resources make it easy to reproduce works without adhering to copyright requirements. Plagiarism and Intellectual Property Rights (IPR) infringements are thus concerns that plague educational institutions. The culture of plagiarism is commonly considered innocuous or even trendy. This is because people are not made aware of the importance of intellectual property law and the consequences of replication.

The problem of plagiarism is quite rampant in India as well. Laws such as Section 51 of the Indian Copyright Act, 1957 exits to solve the problem of IPR violations however the issue of plagiarism has to be reviewed afresh with globalization, information and communication technologies and behavioral factors playing a leading role. In such cases, it becomes imperative for the education system to create awareness and to encourage individual creativity amongst students.
As a part of the paper, a review of the literature was conducted with an interdisciplinary approach including legal as well as a behavioral role to understand the incidence of plagiarism in India. The paper highlights the importance of Intellectual Property Rights in an educational institution (schools and universities) as promoted by Government of India through National Intellectual Property Rights Policy, 2016 and University Grants Commission (UGC) Policy of India, 2018 addressing a concern of plagiarism. Lastly, it confers tools like self- assessment for individuals and a quick checklist to highlight the awareness of academic integrity.

Dinusha Mendis	Bournemouth University	Regulating Mass Copyright Licensing in the Blockchain Era: Myth or Reality?

Since 2008, and particularly in more recent years, much has been written and said about blockchain technology. On the one hand there have been suggestions of it being more than a revolution whilst on the other, it has been regarded as a mere “hype”. Yet, a closer insight reveals that the truth may be found somewhere in between. Particularly, managing Intellectual Property Rights (IPRs) has frequently been viewed as a relevant ‘use case’ for the supposedly ground breaking technology.

This paper will explore the application of blockchain technology within the legal framework designed for copyright. In doing so, the paper will examine the potential for this new technology to strip aside the “middleman” and permit direct transactions between parties. Such elements have much significance for copyright law, particularly from the point of view of enforcement in the dissemination of creative works.

Yet, is such complete decentralisation possible? At the same time, does blockchain technology present us with a new form of registration – and indeed enforcement – which is currently lacking in the online world for IP rights such as copyright. Is blockchain the ultimate solution for copyright law?

Drawing on recent developments, including an analysis of relevant aspects of copyright law, the paper will question the impact which blockchain has on copyright; its relevance for enforcement as well as liability and will respond to the question of whether organisations such as collecting societies have a place in the blockchain era or whether such questions are borne out of a mere hype.

Giulia Priora	Central European University	Are we ready to effectively teach intellectual property law in the age of automated decision-making?

Intellectual property (IP) law is acquiring undisputed relevance in the legal and business worlds. Familiar subjects like patent, copyright and trademark laws, as well as more arcane topics such as geographical indications or traditional knowledge are today part of the academic curricula of numerous departments of law and business studies across the EU and beyond. What some would refer to as the “booming” of IP law [1] may find appropriate contextualization in the structural evolution of academia towards a higher managerial connotation. [2]

The paper focuses on the correlation between the growing significance of IP in legal education and the galloping technological progress. The research question leading the analysis is how the spreading of IP courses can result to be a good step forward towards an effective teaching of law in the next future. With regards to the creative sectors, the future seems indeed characterised by considerable transformations, among which the rising deployment of artificial intelligence (AI), the ever increasing relevance of data, algorithms and related data- driven markets, and the related impact of these business strategies to the public life. To these changes the study of IP law should respond tackling up-to-date legal issues concerning the creation, distribution and access to content and, at the same time, tapping the theoretical premises of the discipline, which imply essential reflections on the social and ethical aspects involved, to stimulate the critical analysis of existing rules.

The paper consists of two main parts, which differ in methodology. First, it will present an empirical research of academic curricula of master degree programs in IP offered by higher education institutions in a selected number of EU Member States (Belgium, France, Germany, Ireland, Italy, the Netherlands, Poland, Sweden, UK). In particular, it will be investigated which specific IP subjects are covered and whether patterns of course design emerge across the universities. Second, the analysis will move towards assessing the effectiveness of detected choices in the IP education

vis-à-vis the set goal of keeping the legal discipline at pace with the time. [3] By so doing, the paper purports to dedicate some reflection on the inevitable changes the legal education is undergoing and draw a lesson from a vibrant field of study and research, which is bringing learning and learners together.

1 E.g. Jeremy Philips, "Intellectual Property: The Boom Continues", Managing Intellectual Property 4 (1994) and by Kenneth Carlaw, David Thorns and Michael Nuth, "Beyond the Hype: Intellectual Property and the Knowledge Society/Knowledge Economy", Journal of Economic Surveys 20(4) (2006).
2 Alberto Amaral, Lynn Meek and Ingvild Larsen (eds), The Higher Education Managerial Revolution? (Kluwer, 2003). A consistent theoretical reflection is proposed by Wendy Brown, Undoing the Demos. Neoliberalism's Stealth Revolution (Zone Books, 2015), Chapter 6.
3 See, among others, Michael Schwartz, Sophie Sparrow and Gerald Hess, Teaching Law by Design. Engaging Students from the Syllabus to the Final Exam (Carolina Academic Press, 2009).

5D: Data Protection (chair: John Morison, QUB)
Edgar Graham Room (2nd floor)

Jiahong Chen Lilian Edwards Derek McAuley Lachlan Urquhart	University of Nottingham Newcastle University University of Nottingham University of Edinburgh	Defence Against Dark Artefacts: Casting Out the Evil in Smart Homes

Cybersecurity in smart homes is notoriously bad. Both informational and physical harms can occur, and as such there are safety considerations too. Internet of Things devices are shipped with poor security defaults, and users often neglect to manage such systems effectively once in use (e.g. setting unique passwords). That is not their fault as usable security is a big problem in computing research, but nevertheless, there is growing interest in finding technical tools to improve device and network security within smart homes. Network analysis tools such as Wireshark provide users granular information about local network activity, traffic data flows from devices which shows how they communicate with other devices and remote cloud servers. MUD profiles of IoT devices provide baseline 'normal' device behaviour, consequently proving a useful tool for understanding exploits, vulnerabilities and attacks that cause devices, sensors and data flows to behave unexpectedly. How this information is shared with users, and when, remains a significant challenge.

Alongside the technical mechanisms, there is an increasingly pressing need to clarify the roles and responsibilities of a range of actors involved in making smart homes more secure. As the home is an intimate space, IoT systems process personal data, but establishing who manages these flows and how is not clear. Home occupants and visitors may have responsibilities, as do those involved in designing, development, manufacture, maintenance and optimisation of devices and also security systems . In this paper, we examine the highly complex technological and legal landscape with the case study of an ongoing multidisciplinary EPSRC research project, Defence Against Dark Artefacts (DADA).

In designing more secure smart homes, a range of legal issues need to be attended too, such as the applicability of the household exemption, the identification of (joint) data controller(s), the selection of an appropriate legal basis for processing, and so on. In the course of these legal analyses, it becomes evident that the current data protection legal framework has placed most of the responsibilities on data controllers, presumably on the assumption that data controllers are best-positioned to ensure a high level of protection of personal data. Yet, as we see the rise of personal information management systems, where users have more control over their data and how it is processed, the roles become more unsettled. In certain use cases, the developer of a technology does not process personal data (and thus is not considered the data controller) but is in fact in the best position to put in place appropriate safeguards. While the potential role of developers and designers in managing information privacy and security exists in GDPR (e.g. Recital 38, Article 25, Article 32), how this translates to practice remains unsettled. The technical, conceptual and practical questions arise with regard to how to fairly distribute the responsibilities among different categories of actors in the context designing more secure smart homes. This paper will begin this process of unpacking and mapping where such responsibilities could lie.

Katerina Demetzou	Radboud University	Risk to the fundamental right of data protection. Lessons to be learned from the Charter-GDPR relationship.

Article 35 of the GDPR introduces the legal obligation to perform DPIAs where processing operations are likely to present 'high risks to the rights and freedoms of natural persons'. The legislature's wording seems to be attributing a broad scope to the concept of risk. This scope suggests that the DPIA is expected to play a crucial role not solely in the protection of the fundamental right to data protection but in the system of protection of EU fundamental rights as a whole. Art 35 GDPR thus presents data controllers with an extended responsibility, which has to be examined in relation to the scope of the GDPR.

Nonetheless, the concept of risk is not legally qualified in the field of data protection. What does risk to the fundamental right of data protection mean? The fundamental right to data protection is found in art 8 of the Charter of Fundamental Rights (the Charter), which is a binding source of primary EU law (art 6 TEU). In art 52, the Charter sets the scope of the fundamental rights by enumerating the conditions under which the limitation on the exercise of these rights is lawful. Case-law from the CJEU with regard to the scope of the right to data protection and with regard to the notion of 'limitation' of the right, will shed light on the concept of risk , which also reveals a tension between processing operations and the right to data protection.

This article will deal with the relationship between the Charter and the GDPR and will answer the following question: "How does the relationship between the Charter and the GDPR inform the interpretation of the concept of risk as a legal requirement for the performance of DPIAs (art 35 GDPR)?"

To answer this question, I will first examine the scope of the right to data protection as defined by the Charter (primary legislation). I will then examine the scope of the right as defined by the GDPR (secondary legislation which has its legal basis on art 16 TFEU). I will ultimately evaluate the relationship between these two scopes. Relevant case-law from the CJEU will play a major role in the present analysis. By examining the scope of the right, valuable conclusions will be drawn as to what a risk to the rights and freedoms mean in the context of art 35 GDPR.

Maria Murphy	Maynooth University	The protection of privacy and the continued role of human rights: Considering the smart city

There is a vibrant debate on the best means of protecting privacy in the present social and economic structure. In addition to discussion of different legal means of protection – from competition to consumer protection law – non-legal means of

protection are garnering significant attention. Notably, the importance of ethics – in particular information ethics – has become increasingly prominent in the public discourse. Many contributions regarding the ethics of privacy have provided invaluable conceptual insight. There has also been some caution expressed regarding the eagerness of many large internet services to adopt the badge of ethics, to the apparent detriment of legal compliance and external accountability. While ethical consideration is vital, this paper argues for the continued importance of human rights law in the modern data processing and surveillance environment.

There have been numerous criticisms of modern human right law. Among these criticisms are the argument that the enforcement of human rights is ineffective, that human rights documents are used as mere virtue signalling, and that where enforced, application is minimal and subservient to government interests. In the privacy context, the criticisms also focus on a notion of outmodedness, where human rights are lagging behind the swift progress of technological development and all the benefits such progress promises. Appreciating the merit in these arguments, this paper argues for the continued importance of human rights documents and institutions for the protection of privacy. Most crucially, such documents provide a framework – with some cross-cultural and democratic legitimacy – to present coherent opposition to government overreach.

In order to illustrate the point, this paper examines the potential role of the European Convention on Human Rights in the smart city context. It is argued that not only does the dialogue of rights provides 'a space for contestation' where rights 'can be rationally discussed', but the ECHR – along with the European Court of Human Rights – has the potential to provide some meaningful constraint on the continued assault on private life. [1] While limited by its supranational nature and the delicate maintenance of its legitimacy, the ECtHR has taken an expansive approach to the interpretation of the scope of the right to respect for private life as protected by Article 8 ECHR. This is reflected in its extensive jurisprudence that recognises many activities – from GPS tracking to DNA databases – as constituting interferences with the first paragraph of Article 8 ECHR. Even though the ECtHR has taken a flexible approach to the concept of 'victimhood' in the surveillance context, it remains that individual cases tend to focus on specific government actions or specific legal regimes. In spite of this, this article contends that the ECHR has a role to play in the evaluation of a much larger and enmeshed system – the 'smart city'.

1. Marko Milanovic, 'Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age' (2015) 56(1) Harvard International Law Journal 81.

7A: Crime (chair: Martin Jones, BILETA Executive)
Room 01/004 (1st floor)

Bela Bonita Chatterjee	Lancaster University	Rogue Robots: Criminal liability for robots who rape?

The advent of sexbots - adult humanoid robots designed for sexual purposes - has prompted many questions, not least whether we might behave well towards them, and what should happen if they are mistreated. Debates on rights for robots in various spheres (eg employment, medicine, social services) are now circulating at academic and policy level. The already-troubled question of consent becomes particularly foregrounded if sexbots are programmed to never to decline advances, or perhaps more controversially, if they are designed to actively resist them, thus simulating rape.

Yet what might happen if they become our sexual aggressors?
How might we conceptualise robotic sexual violence towards humans?

This paper represents a thought-experiment into considering criminal liability for robotic acts of rape. The question posed is of course highly politicised and contested, and perhaps raises more problems than answers: Is such a question appropriate to consider given the current justice gap in human-on-human sexual violence? Can such acts, when carried out by robots, be correctly termed as rape? Would criminal liability make sense in a system designed for people, and what would punishment look like in a system designed around the (dis)comforts of the specifically human body? Drawing on various bodies of work, including debates on killer robots in International Law; Legal personhood; Criminal Law, Criminology and Penology, Posthumanism and feminist technoscience, I invite the audience to think it through with me...

Argyro Chatzinikolaou	Ghent University	Sexual images of and by children: the different degrees of liability of online platforms

Online platforms, search engines, social networks, micro-blogging sites, or video-sharing platforms, mediate the access to and the exchange of information and digital material between internet users. In their role as facilitators of online interactions, however, online platforms may not only host legitimate exchanges, but may also serve as channels for the communication of illegal content. More precisely, internet users might be enabled to access, transfer and download child sexual abuse material (CSAM). In the European Union, concerns about the increasing availability and wide spread of illegal content online have led to the construction of a legally binding framework as well as the adoption of non- binding guidelines and principles concerning the role of internet intermediaries in the fight against the online circulation of illegal content. In particular, whereas the Directive 2011/93 on combating the sexual abuse and sexual exploitation of children and child pornography formulates a legal framework for tackling the online circulation of CSAM, the Directive on electronic commerce provides for exemptions of liability for intermediaries in certain situations.

At the same time, however, research shows that sexual images of children may be also exchanged among young individuals on a consensual basis within intimate relationships or as a form of exploration of sexuality. Alternatively, such imagery may be sent by the depicted child, yet not upon a request by the recipient child and may be possibly unwanted by the latter. In such cases it remains contested whether the produced and exchanged material of sexual nature constitutes illegal content and therefore it may not always be clear whether an online platform could be held liable for hosting or not removing the material in question.

This paper aims to explore the factors which shape the liability of online platforms with regard to imagery and videos of children that carry a sexual element. We hypothesise that there are two [main] factors which may influence the threshold or degree of liability of online platforms; namely, the *nature of the intermediary* (messenger applications and social network platforms; platforms that host pornographic material; illegally operated platforms that exclusively circulate illegal content; search engines; chatrooms or closed groups) and the *nature of the material* (illegal versus harmful versus legitimate; consensual versus non-consensual). Other factors, such as reporting and detection mechanisms in place, or the wording of community standards, will also be explored. Our research draws on EU legal and policy documents as well as legal and social sciences doctrine to shed light on how a long-established approach to liability for illegal online content might be significantly challenged by phenomena (such as sexting) that are not necessarily illegal but still contested in today's society.

References

European Commission (2017). *Tackling Illegal Content Online - Towards an enhanced responsibility of online platforms* (Communication Document, COM(2017) 555 final)
Kuczerawy A (2019). EU Proposal for a Directive on Copyright in the Digital Single Market: Compatibility of Article 13 with the EU Intermediary Liability Regime (December 19, 2018). Bilyana Petkova, Tuomas Ojanen (eds.), Fundamental Rights Protection Online: The Future Regulation of Intermediaries, 2019, Forthcoming. Available at SSRN: https://ssrn.com/abstract=3309099
Livingstone S, Mascheroni G and Staksrud E. (2017). European research on children's internet use: Assessing the past and anticipating the future, *New Media & Society*, 1-20
Walrave M, Van Ouytsel J, Ponnet K and Temple J R (eds) (2018). *Sexting: Motives and risk in online sexual self-presentation*, Palgrave Studies in Cyberpsychology, Springer

Abhilash Nair	Aston University	Criminalising 3D Sexual Representations of Children

UK has one of the most robust legislative frameworks for combating online child pornography, including a simple possession offence for indecent non-photographic representations of children. There is, however, an anomaly in the law in that a country that has criminalised all manifestations of 2D child pornography, including non-photographic imagery,

has not (yet) specifically addressed the possession of 3D sexual representations of children. Whilst there have been some prosecutions against the importation of 3D products such as child sex dolls, using antiquated laws, its possession is not specifically criminalised.

This paper considers the legal implications of criminalising the simple possession of child sex dolls and other forms of three-dimensional sexual representations of children. The paper will firstly outline the rationale for criminalising non-photographic and fictitious child pornography such as CGI and animated imagery, from the perspective of child protection and any harm to children that such laws purport to prevent. Drawing from scholarly debates (that are often cross-disciplinary in nature), the paper will then pose a number of questions regarding the desirability of criminalising the possession of three-dimensional products that depict children in a sexualised manner. The paper will discuss the legal basis for the existing restraints imposed on private conduct in this context, which largely stems from a perceived risk of harm to children rather than conclusive evidence of harm. Developing this further and applying it specifically to 3D products, it becomes apparent that the law is proving to be incoherent and inconsistent in terms of regulating conduct in this area. Notwithstanding the divergent views on criminalising imagery that do not feature real children, it will argue that the law risks losing its legitimacy by criminalising one manifestation of virtual child pornography and not its 3D variants, in light of the particular challenges raised by advances in technology, which render both categories inter-linked from a legal perspective.

Nabilah Ahmad Zubaidi	Prifysgol Aberystwyth / Aberystwyth University	Tackling online child pornography in Malaysia: The challenges to effective enforcement within the 'identification and blocking' strategy

The cases of child pornography involving Nur Nordin in 2015 and Richard Huckle in 2016 caused a sudden shift in the Malaysian government's assessment of the 'internet's stranger-danger' faced by children in Malaysia. These child pornography cases triggered a response from the Government which led to the enactment of the Malaysian Sexual Offences Against Children Act 2017 ("SOAC 2017"). Although legislation such as the Malaysian Child Act 2001 and the Communications and Multimedia Act 1998 providing for the protection of children exist in Malaysia, regrettably, none offers protection from offences such as child abused and used for the making, possession and distribution of child pornography, with the images freely obtainable on the Internet. The SOAC 2017 is therefore timely, seeking to provide for, among others, child pornography offences and their penalties.

Reed argues that a law that cannot be enforced in cyberspace will not command the respect of those who are meant to obey it and is ultimately bound to fail [1]. It follows that the challenge is to tackle effective enforcement of the law in cyber-space, given the global nature of the publication and dissemination of child pornography. Malaysian law enforcement agencies have welcomed the SOAC 2017. There are, however, reports of concerns relating to regulating child pornography internationally, making it a particularly challenging area. Upon the (public-report based) finding of child pornography images, authorities are required to remove such images from the Internet to prevent further distribution or secondary victimisation of the child. While it is relatively easy for the Malaysian authorities to track and remove child pornography for contents hosted within Malaysia, this is less straightforward for contents hosted abroad.

To effectively tackle this problem, a regulatory model of blocking access to child pornography material hosted locally *and* abroad are introduced in other jurisdictions such as the UK, the US, and Canada, via the 'identification and blocking' strategy. This strategy entails the assessment of content by a dedicated body, taking-down the material where possible, and blocking access to Internet users with cooperation from Internet Service Providers ("ISPs"). In the UK, for example, the Internet Watch Foundation (IWF) acts upon reports of child pornography material, requiring ISPs, alongside other law enforcement bodies, to inevitably function as part of the core regulatory framework to block users' access to child pornography contents.

Through semi-structured in-depth interviews with the Sexual, Women and Child Investigation Division (D11) of the Royal Malaysia Police; the national Internet regulatory agency, Malaysia Communications and Multimedia Commission; a local mobile and Internet service provider, DiGi Telecommunications Berhad (PLC), and other stakeholders, this study seeks to gain some insight into the challenges faced by Malaysia's law enforcement and regulatory agencies in tackling the problem of child pornography. Primarily focusing on the 'identification and blocking' strategy, it compares the Malaysian legal and regulatory practices with the UK, the US, and Canada. The paper concludes with recommendations for Malaysia to tackle child pornography enforcement within the above strategy.

1 Reed, C., 2012. *Making laws for cyberspace*. Oxford: Oxford University Press.

7B: Regulation (chair: Gavin Sutter, BILETA Executive)
Stephen Livingstone Room (2nd floor)

Kim Barker	University of Stirling	Social Media Platforms as Fiduciaries: A Utopian Regulatory Benchmark?

The internet offers enormous potential for 'good'. Social media platforms are optimal spaces that are designed to encourage participation, firmly representing not only social and political rights, but also representing the embodiment of equal opportunities. It is then, a travesty that such potential actually serves not to reduce harassment, but instead, facilitate it. Increasing numbers of people are reporting that internet spaces are not safe spaces. Recent studies have shown significant increases in the demographics and level of abuses that are being endured online. Sadly, the legal structures and systems are failing to deal with this phenomenon and are perpetuating the harassment and discrimination now occurring online as well as offline. Rather than the internet providing a platform for campaigning for equality, anti-discrimination, and debate, it is evolving rapidly into a space which is increasingly hostile, particularly for those who dare to be advocates, or dare to disagree. The backlash that is received for speaking out – particularly about issues of diverging opinion – is staggering, damaging, and harmful. This has been particularly evident through debates surrounding Brexit, and the future relationship of the UK & EU.

The so-called 'regulatory framework' for social media platforms, and the Internet landscape more broadly stands in stark contrast to other areas of society which are governed through established legal principles and authorities. This presentation will enrich the current literature by a providing fresh perspective on potential regulatory benchmarks for online platforms, particularly social media platforms by outlining a fresh approach based on the ideal of fiduciary duties. Online platforms collect masses of data and operate cross-border. Whilst individual users are culpable in the use – and abuse – of these platforms, there is a wider responsibility that must be addressed. If platforms are required to act in accordance with fiduciary responsibilities, this may provide a benchmark for responsibility online. This paper will outline such a proposal, especially in light of the proposed Internet Safety Strategy, and the Law Commission Project exploring Online Offensive and Abusive Online Communications. This paper will then assess analyse the potential for such a shift in thinking and regulation through duty.

Paul Bernal	University of East Anglia	Privacy and Fake News

The 'solutions' to 'fake news' have tended to focus on the news itself, whether that be through identifying and labelling or blocking 'fake' news or by placing the responsibility on 'platforms' to remove or otherwise prevent 'fake' news from reaching the potentially susceptible audiences. This, however, is dealing with only the superficial symptoms of a malaise that is much deeper and more pernicious - and more embedded in our information ecosystem and economy. If we are to have a real impact upon the problem it is that ecosystem and economy that needs to be examined - and cleaned up. In particular, it is the failure to protect privacy within the internet ecosystem that is the underlying problem: it makes it possible to identify the kind of fake news most likely to be effective, to identify those who it is most likely to have an impact upon, and then to directly target those people. To make inroads into the fake news problem, therefore, the most important step is to provide better protection for privacy. To make serious inroads into the problem, the internet infrastructure needs to be hardwired for privacy.

This paper will look at both the theory and the practice of fake news, and how the current, 'privacy-unfriendly' internet ecosystem not just supports but encourages it. It looks at both the creation of fake news and its distribution, and how both depend on this ecosystem, from the 'big data' determination of trends and interests and the assistance in creation via Facebook and blogging systems' templates in its formatting and presentation, to the distribution networks that are both mass in scale and micro-targeted, perfect for fake news. It looks at the main current vehicles for fake news – Facebook, Twitter and YouTube – and demonstrates why these are not exceptions or 'rogues', nor are they innocent victims of misuse, but exemplars of a much bigger problem within the internet infrastructure.

The paper will conclude with a look at the implications of this understanding, particularly in terms of finding solutions to the problem. It will demonstrate why the current proposals to deal with fake news, working as they do on symptoms rather than causes (both in terms of creation and distribution of fake news) are likely to be of only minimal effect at best. It will argue that there cannot ever be complete solutions, but that the problem can be reduced in effect by creating a more 'privacy-friendly' ecosystem: making some practices illegal, breaking up internet giants, supporting technological solutions that do not depend on the current systems and so forth. Whether such solutions are possible is another matter: if they are deemed impractical we will have to accept the fake news problems.

This paper will draw upon the work in my 2018 book, *The Internet, Warts and All*, and my 2018 paper in Northern Ireland Legal Quarterly, *Fakebook: Why Facebook Makes The Fake News Problem Inevitable*, but will be new work, taking the arguments made in those works several steps further and drawing broader conclusions.

Francesca Pichierri	FIZ Karlsruhe	Online manipulative practices and the danger to democracy: opening a discussion on regulation

Among many things, *datification* is offering an incomparable opportunity to access, understand and monitor human conduct. Not only more often measurements and calculations are imposed upon operations of the human body (biometric) but also upon operations of the human mind (psychometric). Our thoughts, feelings, actions and behaviours are currently quantified through a powerful integration of psychological and behavioural sciences and computation and are mostly extracted from digital media platforms. As we produce colossal amounts of information online every single day, the Internet has become the perfect place to harvest the data, conduct real-time tracking and predictive analysis.

The effort made by private companies, governments and also scholars to collect behavioural and psychological data about social media users is by now in the public eye. The Cambridge Analytica scandal has further opened people´s eyes. This “effort” seems to respond not only to the need for creating calculable individuals, namely transparent, knowable and predictable but also for creating individuals more amenable to forms of manipulation. After the now notorious emotion contagion experiment carried out by Facebook in 2014, evidence is growing of the sophisticated manipulative practices of technology platforms (for example in the case of the US election or the Brexit vote) which are most of the time difficult to detect as they operate silently and automatically. The need to bring into the open these intentional tactics feels every day more urgent.

Scholars have begun to deal with the consequences and risks of such manipulative practices however, so far, the latter have never been put into a rigorous framework. The following article takes this challenge by focusing in particular on the analysis of manipulative practices in the context of democratic processes such as democratic elections. More precisely, the phenomenon of online manipulation is analysed in the framework of deliberative theories of democracy. As important concerns emerge from these practices, especially in terms of distortion of autonomous choice of individuals which undermines public discourse and democracy, the article concludes by investigating possible solutions against such manipulation. In particular, as surveillance, or more precisely, profiling, makes manipulation possible in the first place, data protection is an area of law that may assume an interesting role in this picture in terms of preventing and protecting individuals against manipulative practices, enable democracy to defend itself.

7C: Google Prize (chair: Ronan Deazley, QUB)
Moot Court Room (2nd floor)

Full papers are available to delegates via the conference website

Claire Bevan	Queen's University Belfast	Regulating the use of Big Data: The Challenge for Government *Discussant: Judith Rauhofer*
MacKenzie F. Common	London School of Economics & Political Science	Fear the Reaper: How Content Moderation Rules are Enforced on Social Media *Discussant: Edina Harbinja*
Róisín A. Costello	Trinity College Dublin	Conflicts between Individual and Intellectual Property in the Digital Era *Discussant: Dinusha Mendis*
Israel Cedillo Lazcano	University of Edinburgh	The Electronic Creation Right *Discussant: Felipe Romero Monero*

7D: Data Protection (chair: Karen Mc Cullagh, BILETA Executive)
Edgar Graham Room (2nd floor)

Trix Mulder Reinder Broekstra	University of Groningen	Does the GDPR have trust issues?

Until now, the processing of personal data in medical practice has been mostly in a closed context, meaning it was clear how the data flowed. The arrival of new technologies, such as eHealth and mobile health, have impacted the way personal data is collected in medical practice. A first review of the General Data Protection Regulation (GDPR) shows that it is mostly drafted for processing health data in a closed medical context. Therefore, this paper analyses where the shortcomings of the GDPR exist in meeting the new, more open context of data processing in medical practice. It is important that this research is being done, since the shortcomings possibly affect the core element, e.g. trust of patients, in the health care system. Furthermore it affects medical paradigms, such as medical confidentiality and informed consent. [1]

Although medical information used to exist in a closed medical context being controlled by governmental institutes, health data now exists in a medical context with commercial organisations playing an important role. Medical practice can use increasingly commercial information technologies for treatment plans and data collection, such as decision support systems, apps and wearables. Moreover, citizens are able to track and acquire their own health data via commercial organisations (e.g. fitbit, 23andme.com). The use of heterogeneous data sources breaks boundaries creating new information flows and risks for privacy. [2] It is, however the question whether the privacy of these data flows are sufficiently protected by the new legal framework of the GDPR.

Article 9 GDPR determines that personal data which are, by their nature, particularly sensitive in relation to these fundamental rights and freedoms, merit specific protection. Health data is part of these special categories of data, since health data comes within a person's most intimate sphere. Unauthorised disclosure may, for example, lead to various forms of discrimination and violation of fundamental rights.

The GDPR prohibits the processing of sensitive health data, unless one of the exemptions mentioned in paragraph 2 apply. One of the exemptions is informed consent, but privacy policies providing the information are ineffective in providing clear information about disclosure. [3] This requires more trust in organisations and the medical context, in particular for health data and collected via (commercial) apps and wearables. Trust which could, for instance, be achieved via an adjustment of the current informed consent practice. One of the options is a more dynamic consent mechanism [4], which this paper will investigate.

Although the open heterogeneous context for data collection brings new opportunities for improving health, the potential lack of clarity in the GDPR and privacy policies put medical paradigms at risk. Aim and use of data collections, limitations of disclosure of information are crucial for the formation of trust in the medical context. [5] As long as the necessary trust is not accompanied by clear checks and balances defining the trustworthiness of organisations and technologies within the medical context, a dangerous game of trust is played that can have unpredictable outcomes for the medical context itself.

1. J.P.A. Ioannidis. Informed Consent, Big Data, and the Oxymoron of Research That Is Not Research. *Am J Bioeth* 2013;1 13(4): 40–42: 40–42; B.D. Mittelstadt, & L. Floridi. The Ethics of Big Data: Current and Foreseeable Issues in Biomedical Contexts. *Sci Eng Ethics* 2015. Springer.
2. S. Barocas, & H. Nissenbaum. 2014. Big Data ' s End Run around Anonymity and Consent. In L. Julia, et al., eds. Privacy, Big Data and the Public Good. Cambridge; New York: Cambridge University Press: 44–75.
3. T. Mulder. Health apps, their privacy policies and the GDPR. *European Journal of Law and Technology*. 2019 (forthcoming).
4. R. Broekstra, et al. Written informed consent in health research is outdated. *Eur J Public Health* 2017; 27(2): 194–95: 194–95.
5. R.Broekstra, J.L. Aris-Meijer, E.L.M. Maeckelberghe, S.Otten, R.P.Stolk. Trust in Biobanking and Big Data: a Qualitative Analysis. *Journal of Empirical Research on Human Research Ethics.* 2019 (forthcoming).

Maria Grazia Porcedda David Wall	University of Leeds	The chain and cascade effects of data crime

An unholy alliance of big data and cloud computing is creating 'upstream', big data cyber dependent crimes. Data crime, such as data and security breaches and malware, is one of such large 'upstream' cybercrimes. Due to the chain and cascade effects, cyber dependent or upstream crimes can lead to cyber enabled or downstream crimes, which massively impacts upon victims.

Based on the discussion of case studies focussing on the UK, this paper seeks to show how several apparently unrelated cyber/data crimes are chained to one another and create a cascading effect of escalating data crime. These upstream crimes later have a secondary impact upon data subjects as 'downstream' cybercrimes such as fraud, extortion, etc., that occur when the data is subsequently monetarised.

The paper will demonstrate that upstream and downstream crimes are often committed by entirely different offending actors against different victim groups, which complicates and frustrates the reporting, recording, investigative and prosecution processes. To do so, the authors rely on a qualitative interdisciplinary methodology of case law and crime script analysis bridging law and criminology.

Taken together, the chain/cascade effects create unprecedented societal challenges that need addressing in the face of the advances of AI and the IoT. The paper discusses how law enforcement agencies can dissuade cyber offenders, and the legal system place adequate incentives, to prevent data crimes in light of the chain/cascade effects.

Matthew Rice	Open Rights Group	Seeking 'quality of law' in the seizure and search of digital devices

This paper seeks to examine the foreseeability standard in human rights law.

As Police Scotland and other police forces across the United Kingdom adopt digital forensics technology in core policing activities such as search and seizure of property, existing legislation is put under strain via the intrusiveness of seizing a digital device against the property that was originally considered in legislative proposals for seizure and search.

According to the European Court of Human Rights, National law must be clear, foreseeable and adequately accessible. Domestic law must indicate with reasonable clarity the scope and manner of exercise of the relevant discretion given to public authorities, so as to ensure to individuals the minimum degree of protection to which they are entitled under the rule of law in a democratic society.

For foreseeability, the test for 'in accordance with the law' is key for human rights assessments, not only to establish the necessity and proportionality of a measure, but also to give the public clarity and foreseeability about their rights. Domestic law must be sufficiently foreseeable in its terms to give individuals an adequate indication as to the circumstances in which, and the conditions on which, the authorities are entitled to resort to measures affecting their fundamental human rights

This paper will seek to explore the standard of clear, foreseeable and accessible in line with search and seizure laws in relation to digital devices, and whether it is achievable given the scale of information available on digital devices and secrecy that is often adopted in the description of these powers. It will use Scotland's legal system as a test case as the issue is currently live and in discussion with the adoption of digital triage units for policing purposes by Police Scotland.

Alongside this the paper will look at modern principles and safeguards to seek to understand what information the public should be given when their device is seized for laws to remain compliant with human rights standards.

Stephanie von Maltzan	Karlsruher Institut für Technologie	Legal aspects of Open Source Intelligence – Predictive Analytics and Data Protection

In the context of ubiquitous computing and Open Source Intelligence (OSINT) a vast array of information has become retrievable with the click of a mouse. This, in turn, has led to new perceptions about how the processed data may be used for Cyber-Security purposes. The use of OSINT is growing significantly. This includes the mining of Social Media Intelligence (SOCMINT). Predictive Analytics as well as Data Mining techniques have enormously expanded the possibilities and the powerfulness of detecting and mitigating risks as they allow managing larger amounts of data and processing them in a faster and more sophisticated way. New strategies for using OSINT are also designed to anticipate national security threats such as international terrorism.

This data analysis requires the processing of several types of data and information that is associated with identifiers, such as IP and email addresses, server logs, which can be subject to stringent rules applicable to personal data and require companies to comply with data protection. Due to the collection and correlation of a massive amount of data, which is inherent to this analysis, particular attention must be paid to the data protection requirements. For most people this data mining takes place without knowing that the data subject is being "profiled". In addition, the Council of Europe highlighted the risk of automatic data processing. Contrary, officials and some legal commentators argue that social media is part of the public domain and therefore anyone is able to access it and justify it on the basis that where users disclose personal data on social media, they do so knowing that the terms and conditions of the social media platforms almost invariably state their data may be shared with others. This does not reflect the reality of social media use. Hence the lack, in the main, of a legal debate around the collection and sharing of OSINT without the consent and usually, knowledge of the data subject. Regardless of the fact that some of the data subjects provide this information voluntarily and that it can be accessed online without significant barriers, it is comprehensively protected as personal data by the GDPR.

It is, thus, of utmost importance to draw the limits of data processing, integrate the appropriate data protection safeguards into the applications and find the right balance between making use of predictive analytics and protecting personal data.

The author intends to explore the issues outlined above and discuss the term "publicly available data" and their legal basis and give baseline examples for Data Protection by Design and Default. Furthermore, the risk of automated decisions and their scope will be discussed. From a data protection rights perspective, the gathering of OSINT demands proper checks and balances.

8A: Crime and Security (chair: John Morison, QUB)
Room 01/004 (1st floor)

Lina Jasmontaite	Vrije Universiteit Brussel	Applications for political asylum in EU Member States: Acceptable limitations on data protection principles and privacy in the times of crisis?

This contribution provides a reflection on the limitations to fundamental rights to data protection and privacy in the context of applications for political asylum. After introducing relevant EU competences and applicable regulatory framework concerning migration and asylum, the contribution delves into data protection and privacy challenges that refugees face when applying for political asylum. Refugees increasingly rely on mobile devices and online platforms to navigate themselves to safe environments. By using mobile devices, they generate large amounts of personal data about themselves and leave digital traces. Such digital data reflecting their journey to safety can be put to use by migration authorities and private companies. While the latter poses numerous ethical concerns over the use of potentially accessible data for developing new business practices, the contribution reflects on the limitations to the protection of personal data and privacy of refugees put by migration authorities when accessing refugees' mobile devices. In particular, the contribution questions the proportionality of measures taken in order to establish an individual's identity or to confirm a narrative presented to an immigration authority. Can and if yes under what conditions migration authorities request refugees to provide access to personal devices and social media accounts in order to speed up the asylum application process? To what extent such policy practices fall within the scope of Articles 7 and 8 of EU Charter and Article 8 of the European Convention on Human Rights? Finally, how compatible are such practices with the EU data protection framework, as revised by the General Data Protection Regulation?

Martin Jones	University of the Highlands and Islands	Legislating for Cybersecurity – A Pragmatic Response to Cybercrime?

The history of the UK response to cybercrime since the 1980s has been largely characterised by three things:

1. Surveys repeatedly indicate that the scale and cost of the problem show exponential increase.
2. The resultant parliamentary furore translates into bespoke new offences and penalties being added to the statute book.
3. The number of prosecutions remain at a relatively low level.

Over time, these components have, in fact, been cyclical resulting in several generations of legislative intervention with questionable success. Recent statistics for England and Wales, indicate that the number of prosecutions under the Computer Misuse Act 1990 is actually on a downward trend. At the same time, data protection legislation increasingly shines a light on security breaches which hitherto may have remained under the radar or at best reported anonymously in a crime survey. This may, over time, provoke further debate as to whether the range of criminal provisions is sufficient and the cycle may repeat.

Yet some provisions, such as s3A Computer Misuse Act 1990, have barely troubled the courts. Despite the noble intention of Parliament in its enactment, it has done little to dent the availability of hacking tools to a motivated individual. The phenomenon outlined above, is not one that is exclusive to the UK though, as it is often mirrored in other jurisdictions. When considered collectively, this calls into question the efficacy of the legislative responses made to date as an appropriate way to tackle the problem of cybercrime.

Against this backdrop, the paper will examine the approach adopted in both the recent Singaporean Cybersecurity Act 2018 which augments existing cybercrime laws and the UK's Network and Information Systems Regulations 2018 which place the importance of cybersecurity on a legislative footing as an important piece of the jigsaw in dealing with cybercrime.

Sandy Sabapathy Rebecca Ong	Hong Kong Polytechnic University City University of Hong Kong	Cyber-security: A Wake-up call for Hong Kong Companies

Cyber-security refers to the technologies and processes designed to defend computer systems, software, networks and user data from unauthorized access and also from threats distributed through the Internet by cybercriminals, terrorist groups and hackers. Cyber-security is one of the most challenging issues facing today's governments, companies and individuals. Cyber threats resulting in data breach are increasing in scope and sophistication at a time when every level of human activity (social, political and economic) is being conducted in the digital sphere. These threats pose an immense cyber risk to organisations and one of their most valuable assets – information. Data breaches to personal information, non- public, business and/or sensitive client and employees' information can have far wide ranging material consequences.

In Hong Kong, the new Companies Ordinance (Chapter 622 of the Laws of Hong Kong) and the Corporate Governance Code have brought positive changes to corporate governance. However, there are no provisions in relation to imposition of standards on companies that control or process data; systems or controls which companies in Hong Kong should implement to reduce cybersecurity risk, and liability and accountability of companies and/or directors in the event of violation of data protection laws. Further, there is no mandatory obligation on Companies whether public or private to report data breach incidents to law enforcement agencies, the Privacy Commissioner or to persons whose data may be compromised by the breach.

The paper has a two-fold objective. First, it seeks to critically examine the current position in Hong Kong on cyber security in the light of EU's new General Data Protection Regulation and China's Cyber Security Law. Second, amidst the tension between secrecy and transparency in cyber security, the paper comparatively examines the US Securities and Commission position and Hong Kong's position on Companies' cyber security disclosure/reporting obligations. Finally, the paper offers recommendations on how cyber risks such as data breaches can be better managed in Hong Kong.

8B: Legal Education (chair: Catherine Easton, BILETA Executive)
Moot Court Room (2nd floor)

Fernando Barrio	Queen Mary University of London	Legal issues with holographic presential distance teaching

The use of holographic technology has advanced from science fiction films to everyday use in several applications, from marketing 3D advertisement to virtual brides in Japan. One of the uses that has been promoted and has attracted much attention is the possibility of using holograms for teaching presentially from distance, what would allow universities and other education institutions to reach students globally with their original location's lecturers. Leaving aside pedagogical considerations, the use of holograms for distance teaching brings a whole new set of legal issues that may impact both the development of distance and presential teaching.

During a presential lecture, a teacher can use a vast array of resources, which include the lecturers developed resources and others that they borrow from other sources, the legal status of them being fairly settled in most cases. However, the digitalization needed to convert a lecture in a hologram and its transmission to different places belonging to different jurisdictions can imply that the legality of the content be uncertain.

In order to introduce a topic or focus the attention of the class a lecturer may make reference to certain topics that are perfectly common and legal in the local country and culture of the educational institution, while the same topics can involve issues that are deemed offensive and or illegal in the jurisdiction where the hologram is played. In the same way the law of the local jurisdiction may consider fair use the reproduction and display of copyrighted material during a class, but its digitalization and transmission may leave that use out of the scope of the legal exception as well as needing the renegotiation and redrafting of the educational licenses. There are also issues related to the ownership of the rights over the content of the lecture itself.

The proposed presentation maps the legal issues surrounding teaching using holographic technologies and analyses in depth the intellectual property implications of such a use in UK, US and Argentina.

Claire Howell	Aston University	Multidisciplinary pairing; a win- win situation

We are today training students for jobs that do not yet exist. We need to encourage innovation and an increased understanding of technology. For innovation to be successfully commercialised it is essential that people working in the STEM subjects have knowledge of intellectual property rights. Do they really get enough knowledge of these rights not only to make them employable but to help them innovate in their future careers? To enhance employability law students need to develop the skills of interacting with clients.

At Aston University we have developed a way of informing Engineering students about intellectual property rights. Law students are paired with engineers. After training in searching the intellectual property databases, law students advise the engineering students about the intellectual property rights associated with the engineers final year projects.

Both law students and engineering students gain relevant and valuable experience, improving their understanding of their subjects and making them more employable.

Paul Maharg Frances Murray	Osgoode Hall Law School	'Dynamic conservatism': second modernity and the digital revolution in legal education

The digital revolution is affecting almost every aspect of our lives, our social structures and bonds, and is affecting the ways that we think about human / machine relations, human / human relations, and our relations with the environment around us. By comparison, there is little engagement in most legal education programmes with digital methods that fundamentally change what we do in those programmes. In most programmes, too, the concept of open educational resources (OERs) is as far from being implemented as it ever was, in spite of studies and exemplar case studies that show the manifest benefits of these approaches to legal education for staff, students and many others involved in the educational process.

In this paper we argue that the need for radical change is more pressing, and that law schools and regulators need to rethink fundamentally their approaches to digital planning for legal education. Using Schön's concept of dynamic conservatism, we point to some of the strategies used by institutions to remain the same by apparently changing (eg nominal change, selective inattention, containment and isolation, and the like) in order to maintain a nostalgic version of the stable state curriculum. We take the case study of simulation, specifically SIMPLE (SIMulated Professional Learning Environment). We analyse the successes and failures of this initiative, the role that OERs could play, and how it fits some aspects of the dynamic conservatism model, and some aspects of Beck's second modernity. Finally, we introduce the SIMPLE 2.0 Project, with its international co-operation, its involvement of regulators, its funding based on sustainable models of finance, and other innovations. We will present the roadmap for SIMPLE 2.0 and some of its functionality at the conference, showing how it takes into account the critical theories of both Schön and Beck.

8C: Intellectual Property (chair: Paulina Wilson, QUB)
Stephen Livingstone Room (2nd floor)

Hayleigh Bosher	Brunel University London	The Human Element in Online Copyright Infringement

The power of technology as a threat to mankind is a popular science-fiction theme, from classics such as George Orwell's 1984 to more recent endeavours such as the haunting TV series Black Mirror. Perhaps the reason for the popularity of this subject is that these stories act as a catalyst to explore the future possibilities of the relationship between humans and technology. Based on our current experience we project into the future expecting technological advances to escalate at an advanced rate. The development of technology is quickly progressing, and that more than ever we are replacing human services with machines and mobile apps.

However, this research aims to bring back the human element in the discussion of online copyright infringement. There are three key instances in which the capacity of a human mind intersects with the development of copyright law. The first is the development of the copyright statutory law, the second is the interpretation of the copyright statutory law by the judiciary, and the third is the cognitive interaction with new technologies by all humans. This research therefore considers the law of copyright infringement at each of these stages.

The use of the internet in copyright infringement is a seminal case study to demonstrate the disconnect between the technological and the human perspectives. This notion of the disconnect between technology and human perspectives translates into the 'internal' and 'external' perspectives of the internet. The external perspective is the technological approach which considers the technical functioning of the computer or access device and the online network. These are the facts of the physical reality, considering the mechanical operation of the hardware and software that makes up the internet as a network. On the other hand, the internal perspective takes into consideration the cognitive understanding of the human experience online. This could also be explained as the virtual reality perspective that derives from the understanding of the internet as equivalent to the physical world. Each perspective determines a different and separate reality which results in a materially different decision when the law is applied to each reality as a set of facts.

These concepts are developed into a Framework for analysis which is then applied to the law of online copyright infringement. The key findings from this research is that the current approach taken in the drafting, interpreting and applying the law attempts to do so from the external perspective. This creates problems such as the law being inconsistent, incoherent and unable to serve its purpose.

The research argues that we cannot forget the notion of the human in the law-making process, or in the application of the law or in the regulating of those who make use of copyright works online. It is people who make and enforce copyright law, people who create copyright works and people who use those works on the internet. As Tim Berners-Lee said: *"The…Web… it's really a system of people….we think of the Web as humanity connected."*

Jade Kouletakis	Abertay University	No man is an island: A critical analysis of the UK's implementation of the Marrakesh Treaty

On the 26th of November 2018, the EU Commission initiated proceedings for infringement of the Treaty on the Functioning of the European Union against 17 (out of 28) Member States for non-compliance with the EU's Marrakesh Directive (2017/1564), with the UK being among them (Pavis 2018, 1). This Directive and corresponding Regulation aims to implement the Marrakesh Treaty and came into force on 12 October 2018, which was the deadline provided to member states in implementing the Directive. Prior to this, the UK government launched a public consultation seeking views on how the UK should approach the implementation of the Directive. This was captured in September of 2018 when the Intellectual Property Office's publication of the 'Government Response to Marrakesh Consultation'. The publication of these findings, coupled with the looming October deadline for implementing the Directive, meant that within hours of said publication the Copyright and Related Rights (Marrakesh Treaty etc.) (Amendment) Regulations 2018 (henceforth 'UK Marrakesh Regulations') were made. These regulations came into force the day before the European Union deadline. The lack of in-depth critical debate around this piece of legislation as well as the EU's announcement of instigating legal proceedings against the UK on the basis of these Regulations underscores the necessity of this paper. This paper seeks to assess the UK's Marrakesh Regulations in light of both the EU legislation as well as similar implementing legislation adopted by what has been expressly identified by the UK as key non-EU trading partners, namely South Africa and the United States. This paper will ask: In light of the Marrakesh Treaty, can it be said that the United Kingdom is displaying the same level of commitment to implementing its international obligations as those with whom they wish to continue trading post-Brexit? In answering this, it will be evidenced that the UK is both acting in violation of Article 10 of the EU Directive, as well as failing to give adequate effect to the spirit and purport of the Marrakesh Treaty, both of which may have significantly negative impacts upon the realisation of human rights by its own nationals as well as external trade relations post-Brexit.

8D: Privacy – and beyond (chair: Abbe Brown, BILETA Executive)
Edgar Graham Room (2nd floor)

Simisola Akintoye	De Montfort University	Cats Against Regulation: Algorithms and Data Protection in the Human Brain Project.

The use of algorithms for decision making is not new, however, the last few years have witnessed the rise of 'big data' and Artificial Intelligence which has seen a growth in algorithms making decisions in virtually every sphere of life including crime management, media, social and economic areas. However, with machine learning comes a plethora of questions, focusing on the decision making process of algorithms and issues around bias and certain categories of people who may be disproportionately affected by the decisions.

With the recent EU General Data Protection Regulation (GDPR) and ongoing debates on algorithms and Artificial Intelligence, effective data protection regulation is timely. Clearly data is being fed into algorithms to function and more data means more efficiency. However, algorithms in their capacity to utilise and exploit datasets and patterns can become biased and flawed as humans go in day to day interactions, the result of which could be catastrophic with recent examples such as Facebook and
Cambridge Anlytica.

Although regulations such as the GDPR focuses on the protection of personal including provisions such as explicit consent requirements and tougher sanctions, the uncertainty remains however for the practical interpretation of some of these provisions in the world of aggregated and analytic algorithmic data.

In view of this, it is the focus of this research to investigate current data protection laws as it relates to algorithmic governance and uncover areas that are yet unclear. Investigation of legal framework as it relates to Algorithms and Artificial Intelligence could inform regulatory reform in scientific research. The research focuses on big data projects such as the Human Brain Project, a Future and Emerging Technologies flagship project focusing on the advancement of neuroscience and brain simulation to understand legal and ethical challenges around developing a regulatory framework that balances the competing interests of privacy and innovation while still maintaining data trust and promoting confidence.

The research is of real world significance to current techno-legal debates on law and innovation, data protection and algorithmic governance.

Edina Harbinja Henry Pearce	Aston University University of Portsmouth	Posthumous medical data donation and privacy – a comparative outlook

As established in research so far, individuals are often not aware as to what happens to these digital footprints post-mortem, and the law and policy in this area are still very confusing and inconsistent (Harbinja, 2017). But what if we shift this paradigm and enable users to employ their altruistic motivations and aspirations by helping them participate in 'citizen's science' and medical research through donating their medical data posthumously (Vayena & Tasioulas, 2015)? This article aims to investigate the idea of posthumous medical data donation (hereinafter: PMDD) from a legal perspective, looking at what the law in the UK and the US could do to facilitate this useful practice in the future.

The idea of PMDD is very similar to organ donation, *prima facie*. Organ donation has been a well-established topic of legal research and medical practice in many countries. The practice has its roots in philosophical, philanthropic and humane ideas and reasons, and the law around it has been developing in the last few decades in particular (Evans & Ferguson, 2014; Skatova, 2011). Data donation would have essentially a similar goal, i.e. to help save human (or other) lives and support medical and clinical practice and research (see the US National Institute of Health, The All of Us Research Program). The aggregation of numerous sets of donated data would support advanced and personalised medical research, providing the basis for data mining, machine learning and AI, which would help generate new understanding of some of the acutest medical concerns that humanity is facing nowadays (e.g. cancer or various mental health conditions, Prainsack, 2014). This, of course, does not come without any risks, such as security, vulnerability of the massive databases, privacy risks for the deceased and their family etc.

This article builds on the helpful findings and arguments introduced by social scientists and humanities scholars in the area (Skatova, Ng & Goulding, 2014; Krutzinna, Tadeo & Floridi, 2018; Shaw, Groß and Erren, 2016). One of the most tangible results of these endeavours is the Code for posthumous medical data donation developed by the Digital Ethics Lab at the Oxford Internet Institute and funded by Microsoft (Krutzinna et.al., 2018). Thus, as research demonstrates, while there may be sound ethical reasons that posthumous data donation is quite straightforward, this is not necessarily the case legally. A legal framework that would support this practice has not been discussed in legal scholarship to date almost at all. [1] This paper is, therefore, a first comparative legal study of PMDD, aiming to address the gap and shed light on the most significant legal issues in the US and the UK that could affect this concept. The focus of this paper is on the US, UK and English law, and the EU, where appropriate. Importantly, the study will look at the general data protection regime, *lex specialis* (sectoral) provisions (legal regimes regulating health-related data, such as HIPAA or the NHS Act), and data governance, thus making some useful parallels and suggestions for a reform of general and sector-specific data protection laws and policies. These changes would contribute to legal and regulatory clarity and coherence and would support the implementation and enforcement of this important and valuable practice. The legal framework would, therefore, go beyond an ethical framework that is considerably more difficult to enforce in practice.

1. For the UK perspective and the basic consideration of PMDD please see Harbinja, Edina, 'Posthumous Medical Data Donation: The Case for a Legal Framework' in L Floridi and J Krutzinna, eds, The Ethics Of Medical Data Donation, Philosophical Studies Series, Vol. 137, Springer 2019		
Judith Rauhofer	University of Edinburgh	Inverse Privacy Harms: The Power of Detriment