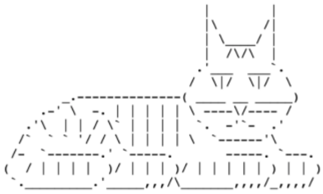

GIKII 2020 ABSTRACTS

AND PIGS MIGHT FLY: THE POWER AND PERILS OF MAGICAL THINKING ABOUT TECHNOLOGY

Dr Paul Bernal, Associate Professor, UEA Law School

Arthur C Clarke famously suggested that 'Any sufficiently advanced technology is indistinguishable from magic'. That observation, increasingly accurate in the current era, has led people, businesses and governments down many perilous paths and has been the cause of many significant problems. This paper will argue, however, that magical thinking, however, *does* have a part to play in the development and use of technology. The questions are when and how should it be used, and what kinds of safeguard we need to prevent setting ourselves on roads to technological disaster.

The paper will use the saga of the NHSX contact-tracing app as a cautionary tale and attempt to map what went wrong and why, in terms of magical thinking, and how it could and should have been done better. It will look at the different roles of governments, technology companies, academia and civil society in this story and try to suggest how each could and should have played their parts differently.

And Pigs Might Fly will draw upon imagery from the films of Studio Ghibli – in particular *Porco Rosso, Howl's Moving Castle, Spirited Away* and *Princess Mononoke.* Studio Ghibli mixes technology, fantasy, history, culture and especially *magic* in ways that can show some of the critical issues dramatically.

Pigs *can* fly, but they generally don't. Expecting pigs to fly, and relying on pigs flying, is a recipe for disaster. If you want your pigs to fly, you need to be willing and able to help them, support them and provide them with what they need. That is as true of technological pigs as real ones.

BATTLESPACE MOON OR FORZA AD ASTRA

Melissa de Zwart

What was that car chase on the Moon all about in Ad Astra? Could it actually happen in real life? Most importantly what guns do they have in space (and why did that guy use one in a space capsule???)?? This paper will combine physics and international law in one lightning fast paper - with added Brad Pitt.

LIVE AND LET DRIVE (OR NO TIME TO DRIVE...THERE'S A LOT OF PUN AVAILABILITY HERE)

Hannah Smethurst

How useful would an invisible car be, really? Would HMRC come after you for unpaid vehicle tax? Do you have to pay and display to park an invisible car, or can you get a permit? What happens if someone trips over it when you've parked it? This paper will look at the real life implications of invisible vehicles, and whether you can avoid the legal repercussions for long enough to....Drive Another Day.

Regulation in Interest-Ing Times

Real Time Law: Lessons from NHSX and FCA

Jon Crowcroft, Researcher at Large

To hide? You have nothing.

It can't have escaped anyone's notice that financial regulation is quite fast at reacting to global epidemic failures of trust, confidence shareholder value etc etc. Of course, some people would really like it if the regulator could be proactive raise there than reactive, but that's a whole other topic. However, in the 2025 novel feline flavivirus pandemic, Prime Minister Cummings decided that he would avoid the fiasco that bought down his predeceessor, and remove the task from the demonstrably useless triumvirate of NHSX, PHE and NCSC, and hand the job of shutting down the pandemic to the FCA. After all, they had experience in sandboxing, chinese walls, and, indeed, full lockdown of the market. All of this is, of course, based in intense, real time monitoring of trades, and modelling of algorithms and interaction protocols, and human behaviour, including all forms of cognitive biases known to man, and a few more known to women. The FCA, as we all recall, managed things perfectly, and the UK survived the pandemic with a mere 1 Million dead, and very little damage to the economy at all, since economic and social distancing were combined into a single incentive aligned, strategy proof system that even the PM was demonstrably unable to undermine, despite multiple expensive attempts.

And so to the present, where the special relationship between President Jolie in the US and the PM has led to the goal of harmonisation of our constitutions and all legal systems. To this end, the FCA was tasked with the idea of replacing both case law history and codified legal framework with a full dynamical system, which acquired its operating rules and parameters simply by large scale surveillance of society, and evaluation of the damage or benefit of actions by individuals and corporatiions, on the health or wealth of other individuals or corporations. No more confusing ethics or dubious human drafted laws based in unexplainable, and indeed, non affordable lawyers' prose. Instead, a single system would now effectively embody Bentham's two ideas, that of the Panopticon and that of Utilitarianism. Objections from the Law Society and Secret Barrista's Association were scorned by the public when it was revealed that the mental health benefits of having cats outweighed the cross-over vital pandemic risks, and could easily be factored into the new social operating system that even China looks at with envy. LAW (Law as an Agency of the Web) went live in June 2026 and took no prisoners.

REGULATING FOR THE APOCALYPSE: I WILL SURVIVE

Lilian Edwards

When we've thought about law in a post apocalyptic movie, its mostly been obvious by its absence. Anyone of the semi-boomer UK generation is forever scarred by the BBCs Survivors series, where our heroes spent what seemed like years avoiding riots, looting, rape(women only) and, for some reason, always hunting down petrol. Soderbergh's Contagion was rather more realistic and accurately spotted that scamming and disinformation might easily be the greatest threats to the rule of law. But in COVID-19 Britain, what we've observed has mainly been a Lot of orderly queuing (surprise) and a viral outbreak of petty legalism and literal interpretation that would make Ronald Dworkin weep. I'll round up a few highlights from recent law including the new version of "No vehicles in the park", why consenting adults can no longer have sex at home and reflect that drafting laws for emergency technologies is actually harder than it looks.

CATS WITH HIGH STANDARDS: ENGINEERS AND THE PUBLIC INTEREST

Alison Harcourt

The increasing shift away from national regulation to problem solving via interoperable technical standard agreements renders key developments in the Internet's architecture immune to public interest campaigns. Although public interest concerns have long been recognised by SDO participants, efforts to mitigate this occur around the fringes of main SDO work and are mainly initiated and carried out by civil society, academics, and specialist groupings. Public campaigns by the EFF, a *New York Times* investigation, and recent action by the FTC and the UK parliament are resulting in more public recognition of the problem. However, serious address of the problem cannot come about without the recognition and direct promotion of certain Internet rights within SDOs through existing international legal agreements. This presentation discusses these options with discussion of recent developments within the UN Human Rights Council, World Economic Forum and OECD and how to translate these tools into SDO decision-making.

‘Oh it’s true, it’s damn true!’ Can kayfabe help us wrestle with the regulation of disinformation?

Miranda ‘Purple Peril’ Mowbray and Tristan ‘Crazy Rich Bayesian’ Henderson

This talk is about the phenomenon of consensual fakery in professional wrestling. In professional wrestling circles, the word *kayfabe* refers to the scripted and choreographed nature of the performance that is presented as though it were a real sporting contest, and to the action by performers of remaining in character both in and out of the arena. The journalist Michael Brick described kayfabe as a type of advanced method acting: although ‘you know you’re faking and the audience knows you’re faking and you know the audience knows you know you’re faking’, you keep up the act both during and after the scripted performance.[1]

Professional wrestling fans know very well that matches are pre-determined, however they too pretend that they are real, and suspend their disbelief. A grown fan may cry for joy as a result of a match that he knows is theatre rather than sport. In addition to acting out scripted physical moves in character, performers have fake backstories, and the fictional feuds and romances that form part of the plot are also a subject of kayfabe. In May 1987, ‘Hacksaw’ Jim Duggan found himself sacked from the then World Wrestling Foundation after being found travelling together with the Iron Sheik in a car. Being arrested for marijuana possession was only part of the reason; as enemies in the WWF kayfabe, they ‘weren’t allowed to travel in the same cars together’.[2] New developments such as social media are used to augment kayfabe,[3] which can make it harder for performers to sustain the illusion. But at the same time audience participation through campaigns such as #HijackRaw allows fans to shape the kayfabe themselves – are the audience prosumers or co-regulators?

Wrestling, the law and ethics are highly intertwined. The existence of kayfabe was confirmed in a New Jersey Senate hearing, and made the front page of the New York Times.[4] It has been argued that kayfabe has been used to shape American norms and values.[5] There are also some intriguing links between professional wrestling and politics. Donald Trump has been involved with professional wrestling since at least 1988, when WrestleMania IV was staged in the Trump Plaza Hotel in Atlantic City, and he is one of only two non-wrestlers in the World Wrestling Entertainment (WWE) Hall of Fame. In 2007, Trump took part in a brief scripted fight with Vince McMahon, the owner of WWE, on the floor just outside the ring during a match. According to Travis Waldron, who interviewed several people involved in the show, Trump landed his blows on McMahon for real rather than following the planned choreography.[6] Had Trump fallen for his own kayfabe? Do political supporters of Trump (or of The Great Sasuke or Jesse ‘The Body’ Ventura, both of whom were elected to political office) practice kayfabe with regard to politics? Nick Rogers suggests that ‘Donald Trump rode kayfabe from Queens to Trump Tower to *The Apprentice* to the White House.’[7] So what can we learn from kayfabe when designing technical and legal responses to online deception? What does this imply for the regulation of political disinformation?

In Lucha Libre, the Mexican version of professional wrestling, the name for the good-guy wrestlers is *técnicos.* The word *técnico* means someone who is technically proficient and relies on skill rather than cheating to win. Professional wrestling, therefore, is a popular dramatization of the struggle of the law-abiding geeks against the forces of evil. What could be a more appropriate topic for Gikii?

Our title refers to Kurt Angle's catchphrase – this Olympic gold medallist turned from amateur to professional wrestling, and was only offered a WWE contract once he agreed to participate in kayfabe.[8] This presentation will be given by the *técnico* tag team of Miranda 'Purple Peril' Mowbray and Tristan 'Crazy Rich Bayesian' Henderson.

[1] Michael Brick, 'Jingo Unchained' (*Harper's Magazine*, 5 January 2013) <https://harpers.org/archive/2013/05/jingo-unchained/> accessed 28 May 2020; quoted in Gary Smith, '"Why's This So Good?" Michael Brick and Jingo Unchained' (*Nieman Storyboard*, 30 June 2016) <https://niemanstoryboard.org/stories/whys-this-so-good-michael-brick-and-jingo-unchained/> accessed 28 May 2020.

[2] Josh Coulson, 'Remember When: Jim Duggan & Iron Sheik Almost Killed Kayfabe By Getting Arrested Together' (*The Sportster*, 12 January 2018) <https://www.thesportster.com/news/remember-when-duggan-sheik-kayfabe-arrested/> accessed 27 May 2020.

[3] Eliseo Sciarretta, 'The Use of Social Media as Part of a Transmedia Storytelling Strategy in WWE's Professional Wrestling' in Gabriele Meiselwitz (ed), *Social Computing and Social Media Design, Human Behavior and Analytics*, vol 11578 (Lecture Notes in Computer Science, Springer International Publishing 2019).

[4] Peter Kerr, 'Now It Can Be Told: Those Pro Wrestlers Are Just Having Fun', *The New York Times* (10 February 1989) <https://www.nytimes.com/1989/02/10/nyregion/now-it-can-be-told-those-pro-wrestlers-are-just-having-fun.html> accessed 27 May 2020.

[5] Sam Migliore, 'Professional Wrestling: Moral Commentary Through Ritual Metaphor' (1993) 7 Journal of Ritual Studies 65.

[6] Travis Waldron, 'The Definitive History Of That Time Donald Trump Took A Stone Cold Stunner' (*The Huffington Post*, 15 February 2017) <https://www.huffpost.com/entry/donald-trump-wwe-wrestling_n_58a35601e4b094a129ef8c46> accessed 27 May 2020.

[7] Nick Rogers, 'How Wrestling Explains Alex Jones and Donald Trump', *The New York Times* (25 April 2017) <https://www.nytimes.com/2017/04/25/opinion/wrestling-explains-alex-jones-and-donald-trump.html> accessed 27 May 2020.

[8] Josh Barnett, 'From Mat to Ring, WWE's Amateur and pro Wrestling Connection' (*USA Today*, 5 February 2017) <https://www.usatoday.com/story/sports/2017/05/02/wwe-olympic-wrestling-ncaa-kurt-angle-brock-lesnar-chad-gable-jason-jordan/100825750/> accessed 28 May 2020.

Speech is Circular: Twitter (/Facebook), Trump and the Public Interest

Elettra Bietti

Jack Balkin argued that free speech is a triangle. While the old model of free speech was dualist and entailed two kinds of actors, governments on the one hand and speakers on the other; today's speech for Balkin must be conceived as a triangular model that involves (a) governments, (b) privately-owned infrastructures, including social media companies, search engines, broadband providers, and (c) speakers.

A series of recent events, particularly Twitter and Facebook's treatment of US President Donald Trump's inflammatory tweets on elections and the Minnesota protests, have crystallized enduring and heated debates around online free speech, content moderation and the role of platforms in enabling and moderating the spread of harmful speech by politicians. Looking closely at the stakes of the debate, online speech is more than a triangle. The discourse around online speech forms an insoluble circle that needs to be broken.

The task is not to identify bad actors and good actors, to focus on limiting or enhancing their individual ability to engage in speech or regulate it. It is instead to realize speech's connectedness and embeddedness in other social, technological, legal and political factors, and to limit political and other communications' reliance on profit-motivated infrastructures that channel speech in ways intended to maximize user-engagement, addiction, behavioral targeting, and polarization.

https://medium.com/berkman-klein-center/free-speech-is-circular-trump-twitter-and-the-public-interest-5277ba173db3

Zombie technology in the twilight zone: Why polygraphs refuse to die

Kyriakos N. Kotsoglou (Senior Lecturer), Marion Oswald (V-C's Senior Fellow) and Daniel Robinson (3rd year LLB student), Northumbria University

Polygraphs are becoming the new (ab)normal. Despite existing in a 'twilight zone' reserved for disputed science, the polygraph (or 'lie detector' as it is commonly called) is a technology that refuses to die. On the contrary, polygraphs are enjoying a resurgence in England and Wales, as a weapon in the probation service's armoury to manage the 'risk' posed by an offender. For several years, polygraphs have been used in the monitoring of convicted sex offenders on licence (Offender Management Act 2007). The current Government now proposes similar polygraph schemes for convicted terrorism and domestic violence offenders, following evaluations claiming that offenders who are made subject to polygraph testing are likely to disclose more information than before.

This paper is not really about how the technology 'works' (because it doesn't!). Even one of the early 'inventors' of the polygraph, Leonard Keeler, admitted that there is no such thing as a lie detector. Our concerns centre around how the polygraph's output (i.e. physiological data) are interpreted and instrumentalised in order to extract adverse statements from the interviewee.

The central claim for the polygraph –that the polygraph can indicate deception – is linked to the disputed (and many would say, discredited) assumption that deception can elicit physiological responses in a consistent and reliable way. We will show – including through information obtained from FOI requests submitted to UK Police Forces and the Ministry of Justice - that the use of the polygraph faces all the usual problems, familiar to both evidential contexts and the use of machine learning: lack of validity, lack of consistency, lack of transparency and the need to use deception and psychological manipulation in order to convince the subject that the polygraph works (via the pre-test, alias 'stimulation' test). We will highlight the inadmissibility of the polygraph in criminal proceedings, the discouragement of its use in police investigatory processes, the ‘oppressive’ nature of the test and the pressure on the offender to comply with the process. Probation officers, however, can use an indication of deception in test results, and the offender’s reaction to the test process, to initiate further investigatory or intrusive action which could ultimately result in the recall of the offender’s licence based on an assessment of the offender’s risk. (A ‘no deception indicated’ result is taken to mean that the offender is complying with their licence conditions despite the significant doubts over the validity and accuracy of the polygraph, which leads to undetected risks to the public and complacency). This creates, we will argue, a major contradiction which is detrimental to the integrity of the legal order and raises questions on human rights grounds.

Brains, Bodies and What Comes At (Out) the End

No one speaks the language his brain now speaks”: Legal responses to neurotechnology for communication

Jennifer Chandler

Detection of covert or imagined speech directly from neural signals is opening up possible avenues of communication for people with a range of mobility impairments, and perhaps even damage to other parts of the brain circuitry involved in producing speech. The law is used to challenges with linguistic compatibility, but has struggled in some cases with forms of augmented and assistive communication. Issues related to testimony in court, consent, responsibility for harmful speech, and privacy of thought and communication are posed by these novel forms of communication intermediary.

The Ethics of Brain-Computer Interfaces

Kipp Freud

Brain-Computer Interfaces (BCIs) are systems which allow users to interact with technology directly using their brain activity. These systems are becoming more commonplace in today’s world; they are being used to control prosthetic limbs, to predict incoming seizures in epilepsy patients, and are beginning to gain traction in video game control. Research is currently being undertaken to utilise BCI technologies for military purposes, with DARPA recently investing $18 million in the MOANA project, which is aiming to achieve direct brain-to-brain communication within 4 years. It seems that not only will these systems be used to improve the lives of the ill and disabled, but also to enhance the physical and cognitive abilities of man to super-human levels.

This talk will be a whistle stop tour of the potential ethical quandaries surrounding the incorporation of BCI technology into our world. For instance, should predictive or “autopilot” components be added to prosthetic limbs? They have been shown to hugely reduce complexity and increase the ease of use of such systems, but who should be accountable in the case of an accident caused by a wrongly predicted action? Some intrusive BCI technologies have been shown to dramatically alter the personality of the user - should close family members be able to demand the removal of these technologies without the consent of the user, owing to the fact that they’re no longer “themselves”? Must soldiers implanted with BCI technologies enhancing their abilities be required to have these systems removed upon discharge? Doing so may cause huge mental hardship for the soldier, but could allowing enhanced humans to mix with society create a divide between enhanced and non-enhanced?

Richard Nixon Burgers ™ Trademark law, WTO and the regulation of cultured meat

Mariela Eletti de Amstalden, Burkhard Schafer

In “The State of the Art” Iain M Banks describes a macabre dinner on board of a Culture Ship, in orbit around 20th century earth. The host managed to extract one cell each from the worst dictators plaguing mankind. Put into the lab that grows the food for passengers and crew, he grows a variety of meals from these samples, serving the bemused party goers General Stroessner Meat Balls and Richard Nixon Burgers, Ferdinand Marcos Sauté and Shah of Iran Kebabs, Fricaséed Kim II Sung and Boiled General Videla, among others.

But what, exactly, have the party goes been eating? Marcos and Nixon? Something that is part of either, and therefore human? Or is what was created in the lab a new entity, one that does not fit easily in conventional ontologies? The answer to this question has obvious legal ramifications, from prohibitions of cannibalism, dietary laws of various religions, food safety and labelling, and with that also marketing and trademark law.

We will use the Bank's story as a lens to explore some of the legal issues that cultured meat is bringing to the regulatory regime. Promoted as an environmentally more sustainable alternative to farmed meat, research into cultured meat has gained new urgency in response to the climate catastrophe. Nonetheless, the regulatory push back from established market players, in particular the farming industry, is already noticeable. Our analysis will focus on what may be seen as a more arcane legal issue, the question of trademarks for cultured meat. We will show however who this question raises some of the deeper philosophical issues – a rose by any other name does not quite smell as sweat as neuroscience research has shown, and how the new food will call itself, or be allowed to call itself, will have significant impact on its market acceptance. Cultural and anthropological practices around meat and its consumption add another layer of difficulty, especially for international legal regimes.

DATA IS THE NEW SEWAGE: TOWARDS AN ACCOUNT OF EXCREMENTAL PRIVACY

Reuben Binns

The status of poo in the theory of privacy and data protection has, to date, left nothing more than the occasional skidmark [1]. This blindspot is understandable, given the intensely private, and purile, nature of the subject. However, it may soon float to the surface as an influential (and effluential) topic of study.

Not content with mining data from our phones, wearables, and credit cards, the AI-hucksters have identified a new fertile ground. Boston-based company Biobot is "the first company in the world to commercialize data from sewage", rendering populations legible by poop. While the potential for poo as a source of biological power (e.g. via methane extraction) has long been recognised, its incorporation into surveillance assemblages may also present new forms of Foucauldian biopower, which merit scholarly attention.

In this talk, these themes will be explored through the lens of po(o)p culture, in particular the pile of poo emoji, whose semiotics are, thankfully, increasingly divorced from its faecal connotations.

Poo presents several vexing questions and case studies for privacy and data protection law. Aside from the quintessentially private nature of the act of its production, it is also renders its producers highly identifiable. The gut contains over five hundred species of bacteria, some of which are individually unique. Furthermore, it will often reveal information about the physical health of those identifiable individuals, and is therefore 'special category data' (or 'SCat' data for short).

Bearing in mind such scientific possibilities, modern sewage systems present only partial privacy protection for those who use them. And even if stool-based re-identification is inherently messier than equivalent digital methods, aggregate wastewater analysis may still enable the inference of otherwise unquantifiable vices at the group level, as evidenced by countless studies of levels of cocaine in London's wastewater.

This may also prompt us to reflect on new metaphors; rather than metaphors of data as oil, gold, or silk, perhaps data is better compared to sewage. Various influential (and less effluential) water-based vocabulary already abound in enterprise data management; data 'streams', 'lakes', or 'plumbing'. Data as sewage flushes away such guff and brings to our senses the effluvia of technology discourse in recent decades. Data is less a resource to be commoditised, than a daily bodily emanation to be contained, transformed and ultimately safely disposed of or recycled. Its safe handling is a public good, and is probably best handled by at least partially municiple infrastructure. The sceptic tank will only function so long before it bursts.

Footnotes:

[1] One notable exception is Haddadi, Hamed, Tristan Henderson, and Jon Crowcroft. "The ambient loo: caught short when nature calls?." ACM SIGCOMM Computer Communication Review 40.2 (2010): 78-78. The author notes the travesty that this paper has only one previous citation. The author is also pleased to observe that this means the present citation is citation Number Two.

The Internet of Antipodeans (+1)

The Internet of Singhs: the pani^ of managing one's identity online

Jat Singh

Much of what we use online is linked to an identifier. As more and more applications and services become available, bringing more and more aspects of everyday life online, more and more accounts and profiles are created. In many cases, a 'fake' (or mistyped) email or phone number is enough to move forward with using a site or service.

But what of those whose accounts are created in their name? What does this mean for those at the other end of this seemingly 'random' profile - the holder of that email, the holder of that phone number. For those individuals, it can be quite the struggle to have such things rectified. Rights and law, maybe... but what does this mean on the ground?

Towards this, this paper will explore the practicalities of identity management in situations when you're linked with someone else's account or profile, based on examples from my own experience of holding a gmail address. Using a series of anecdotes – spanning from bank loans to marriage proposals -- I'll highlight the pain in dealing with correcting this stuff, which can entail anything from a simple 'click 'n fix', to begging, and even taking matters into one's own hands. The risks and implications re current approaches for rectification are considered, as part of a broader argument for more attention to be brought to the area.

Your Health and Fitness Data Can and Will be Used Against You

Dr Andelka M. Phillips

https://www.andelkamphillips.com

Track your fitness. Track your health. Track your digital life. Sequence your genome. Businesses want our data. The police want access to that data too. Other entities also want that data.

Nothing could go wrong right?

A wide range of consumer focussed health care services are changing our lives. The personal genomics industry has created a market for DNA tests as consumer services, while wearable tech allows us to track our health in new ways. However, most of these services are not standardised and may provide consumers with contradictory results. Some services may also not be completely reliable and all of these technologies pose privacy and security risks. They may also pose risks that we might not anticipate, as our data is collected and used for secondary purposes often without our knowledge. This brief talk will provide an overview of privacy and other risks in relation to the secondary use of data collected by personal genomics and wearable technology companies.

Litigating about Information Technology when the (Tribunal) World is Seemingly Flat

Dr Reuben Kirkham, Monash University

Over the past five years, I've had what might be said to be a strange experience. It all started with a Freedom of Information Act (2000) request I made back in 2014: the response I got was in effect that 'computers don't work' and thus it will take us too long to find the information (and my request was rejected under s.12). Curiosity perhaps got the better of me and so I challenged that decision all the way to the Upper Tribunal. I lost that particular case, but the result of that case was for the Upper Tribunal (perhaps unwittingly) to rewrite the Freedom of Information Act (2000) system to be more favourable to information requesters.

My experience of the Information Tribunal system has been an interesting and ongoing journey. Throughout my more recent interactions with the Information Tribunal and 'senior Tribunal Judges', I have 'learned' some interesting things. Microsoft Excel, apparently, can only be operated by an 'academic computer scientist', as opposed the Information Commissioner's Office. I have also been told its impossible to record interactions with computers and thus they cannot be demonstrated in a court room (I wanted to show the Judge that using Microsoft Excel was accessible to the general public): indeed, I was apparently 'unreasonable' to even trouble the Tribunal with such a request. I was also informed that computer security practice should operate on the basis that all staff members can be trusted, rather than being on the basis of protecting personal information from an organisation's employees. At the same time, this Tribunal (with the support of its Chamber President) also asked me to prepare a signed printed copy of an email I had forwarded, just in case I had forged it.

This talk will be a tragi-comic (yet true) story of how such things can happen in a tribunal which is supposed to specialise in Information Technology. I will also look to the future: what can we do to stop something like this happening again? How can we ensure fair trials for matters relating to information technology? What qualifications does a Tribunal really need to have to fairly hear such cases? These problems thus represent important concerns that need to be addressed in a serious manner going forwards.

The PETs Are Coming, Oh, God, Please, Listen, You Have To Stop Them Befo—*scream* *ominous thud* *white noise*

Michael Veale, University College London

In the dark platform years of the early 21st century, sensitive data was hoovered up, stored and hoarded in vast, secretive data centres, with its use sold to the highest bidder. Elections were snatched, prices fluctuated before people's eyes, creepily appropriate products inched their ways into the timelines of unsuspecting citizens, and people's emotions were manipulated on an unprecedented scale.

In the face of this adversity, a plucky band of activists, researchers, idealists and technological architects sought to reshape and rethink it all. They came with new, cryptgraphic technologies which, it was promised, would allow society to have its cake and eat it. Citizens could benefit from a more informed world, and reap the societal gains that came with the rendering it legible and computable to worthy folk such as public health authorities, cancer researchers, and meme scholars. They wouldn't have to give up their privacy. They wouldn't have to give up anything. Technologies such as multi-party computation, homomorphic encryption and differential privacy would underpin this new world, and a new, decentralised era would be born again.

This plucky band lost.

In fact, they didn't just lose, but they actually ushered in a new, and more dangerous form of control, one which became even more difficult to resist, and which technology and the law could do little to stop dividing and manipulating society to the advantages of the powerful.

This is the story, sent from a few years in the future, of exactly how they lost. It was thrown back in time on the last, unencrypted piece of technology — a ragged Betamax tape - by a renegade cryptographer-turned-critical scholar, drawing upon the abundant sources of energy required by home of the encryption to open the space time continuum. She sent one last, desperate plea:

The PETs Are Coming. Stop Them.

What did she mean? And is the future that she lives in and comes from inevitable? To make sense of her message we must get into the mind of the proponents of privacy enhancing technologies, or PETs: both those that dream of their use for a better world, and those who seek to use them to reify their power. Will they help us or harm us? Or is our focus on privacy a huge cat-egory error? And importantly — are we too late?

E.(R.)T.: FROM PHONE HOME TO VIDEOCALL SCHOOL

Rossana Ducato (UCLouvain), Giulia Priora (Scuola Superiore Sant'Anna), Chiara Angiolini (University of Trento), Alexandra Giannopoulou (Institute of Information Law (IViR), Bernd Justin Jütte (University of Nottingham), Guido Noto La Diega (University of Stirling), Leo Pascault (Sciences Po Paris), and Giulia Schneider (Scuola Superiore Sant'Anna)

The rapid spread of the SARS-CoV-2 virus in the early days of March 2020 shut down universities in most European countries. With the exception of those already offering blended teaching activities, the swift move to Emergency Remote Teaching (ERT) took most universities by surprise. Some universities were able to rely on licensed software that was repurposed to instruct students and to provide their staff with appropriate training. Others left it to their teachers to identify software and IT services for distant learning purposes. In both scenarios, institutions and teachers had fairly little time to assess the suitability of the online tools with the required attention. As preliminary data are showing, the use of videoconferencing and e learning platforms under ERT circumstances raise several concerns in terms of data privacy and copyright.

The paper intends to shed light on the major critical aspects and potential "creepy" functions hidden in the jungle of terms of service and privacy policies of online services used for ERT. The main goal is to verify whether sufficient and clear information is provided, in order to enable teachers to carry out educational activities and interact with their students without uncertainties as to the potential legal consequences of their use and concerns regarding the protection of their content and personal data.

To this end, the paper examines the terms and conditions, privacy policies and community guidelines of a sample of nine online services used across Europe to deliver ERT. The selected tools include dedicated software for managing teams and groups of students online, content sharing platforms and social networks, video-communication services repurposed or retrofitted to answer the needs of education.

MEMES AND PARASITES: ANALYZING DISCOURSE ON THE COPYRIGHT DIRECTIVE

Amy Thomas and Ula Furgał CREATe Centre, University of Glasgow

The Directive on Copyright in the Digital Single Market has been a subject of heated and highly polarised debate, and an object of intense lobbying from the outset. It grasped the attention of a multitude of stakeholders, including tech companies, publishers, platforms, creators and SMEs, and urged thousands of people to go out on the streets in a sign of protest against what they believed was the "end of the internet as we know it". The debate was often emotional, and involved such terms as "meme ban", "censorship", "upload filters", "link tax", or a puzzling "value gap". However, amongst those emotive catchphrases lies a foundational discussion on the purposes of copyright law, and how its relationship with artists, technology, media, news, culture and citizenship unfolded.

In this presentation, we investigate how discourse developed during the negotiation phase of the Directive, focusing on the most controversial provisions: Articles 15 (press publishers' right) and 17 (platform liability). We conduct a discourse analysis of (1) parliamentary debates, (2) press releases by the Commission, Parliament and Council, and (3) 80 stakeholder submissions that sought to shape the evolving legislation. We also offer preliminary observations on public engagement with this highly technical debate through an analysis of Google search trends and Twitter data, including (cat) memes and viral video clips.

Through discourse analysis, we uncover four themes that appear to dominate the debate: (a) Technocratic (responding to tech development by updating copyright framework), (b) Value gap (redistribution of revenues to benefit creators and producers), (c) Internet freedoms (freedom of expression and user interests), and (d) European (promotion and protection of European culture and identity). Finally, we show that changes in the Directive's text can be associated with the appearance and evolution of these themes, but that these changes are in form only, rather than in substance.

Presentation is based on the paper "Copyright in the Digital Single Market: A discourse analysis of law making (2016-2019)" by Ula Furgal, Martin Kretschmer and Amy Thomas (work in progress).

Living in the (Smart, Bugged) City

The Internet of Best Bodies

Andrea Matwyshyn

In the movie Gattaca, a dystopian society is governed by technologies that engage in DNA curation. Only the "best" people have access to economic opportunity and the full panoply of rights. Is Gattaca merely a fictional darkest timeline, or is it our inevitable future? Examining the intersection of eugenics history and technology reveals an uncomfortable set of truths: policymakers and builders have sometimes wielded terms such as "innovation" and "progress" to justify culling society of "undesirables" and preserving "purity." In other words, these terms of "innovation" and "progress" have historically sometimes reflected particular visions of the "right " kind of human bodies and used "scientific" hyper-quantification through various technologies as justifications for bigotry and exclusion codified in law. Using the case study of the 1933-1934 World's Fair, this work argues that as the Internet of Bodies combines with the "Extended Body Processing" of machine learning, assumptions about which bodies are "correct" will be implicit in these technologies and in their derivative policy decisions. They threaten to birth a 21st century variant of eugenics in the name of "innovation" and "progress" – a dark timeline that should be vigilantly avoided.

Stay at Home (Network), Protect the N(ational) H(igh-priority) S(ystems), Save (Actual) Lives: Regulatory Considerations for Isolating End-of-life Consumer IoT Products

Jiahong Chen

The strategies of managing cybersecurity risks are perhaps not that much different from handling threats to lives in a global pandemic after all: Identifying those who are infectious or vulnerable, and cutting off their contact with others. In cyberspace, IoT devices that are no longer supported with updates from vendors are especially vulnerable – and potentially dangerous, as they can be exploited to attack other connected devices or even the infrastructural network. Incidents of botnets targeting hospital systems have shown that keeping compromised IoT devices off the internet could be a matter of life or death. Indeed, the health sector has been given the highest priority under the NIS Directive as a key area where the essential operators are regulated.

To improve cybersecurity of consumer IoT products, both the draft European Standard (EN) 303 645 and the UK's Regulatory Proposals have set out the requirement that the period for which the product will receive security updates must be explicitly stated. However, neither of the initiatives has further specified what should happen upon expiry of the support period, when the products are no long safe to stay connected. This raises the regulatory issue whether the disconnection or even phaseout of end-of-life consumer IoT products should be regulated.

As with the controversies surrounding the measures taken to fight the current pandemic, any governmental attempt to regulate the end of IoT product support will inevitably spark debates on individualistic freedom vs collective safety, and also libertarianism vs paternalism. On the one hand, the device owners' right to property could arguably mean that the functionality (including connectivity) of the products should not be interfered. On the other hand, however, leaving a large number of end-of-support devices unregulated may pose an enormous threat to the safety of critical infrastructures.

This paper will examine a range of legal and technical solutions and compare the strengths and weaknesses in terms of their regulability. These options include alerting consumers, mandatory recycling by retailers, planned offlining by manufacturers, and by-default disconnecting by smart hubs. Policymaking in this field will be subject to certain techno-economic constraints but there is an increasingly pressing need to start public discussions as more and more IoT devices are left insecure online.

Controlling actions and words, from the view of City of Silence.

Fernando Barrio, Queen Mary University of London

"The year was 2046. The place the Capital of the State". A time and place where the omnipresent state controlled every aspect of the citizens behaviour, including their words. The technique was not new, but somehow original; instead of prohibiting certain types or categories of expression, the State decided the list of words and topics that could be used. No place for ambiguity, no need for interpretation.

The scenario presented by The City of Silence, the science fiction short tale of Chinese author Ma Boyong, takes to a new level the use of information technology to control and monitor citizens actions, and bring into question the discussions taking place in the quarantined 2020, a collection of very Gikii-like discussions.

Ma Boyong plays homage to Orwell's 1984, it is the book that the rebels read when then get together in a lead cladded house to speak freely, and, in extreme and exaggerated form, engages with the issues that society is facing today.

A simple search for jobs during the pandemic shows that almost all social network platforms are hiring content moderators in any possible language. There are daily calls to control what those in power can and cannot say in social networks. The need to restart a life with a distant resemblance to normality seems to be based upon the development of technological tools that would enable the state to know the health statues of every citizen in real time, while watching where that person citizen goes and who is meeting with.

Through the also fictional analysis of The City of Silence with today's legal framework that regulates the use of personal data interlinked with the rules that organise what can and cannot be said in the public sphere, including the privately own social networks, the presentation looks to deconstruct that situation of the State towards the present, where the policies in place or in discussion could lead to that scenario.

How compliant with the GDPR is the request of the State to know every step taking for the citizens of the City? Will that be justified in times of a pandemic? How far does the freedom of expression goes, while the expression contains no opinion but false and distorted facts? Who is the arbiter of the exceptions?

Western democracies seem to keep finding reasons, valid or not, to increase the surveillance of actions and words of its citizens, moving closer to China, where the situation has gone further in that direction and, contrary to what many Western analyst imagine, with a high degree of support from the population. Seeing today from a Chinese prism of 2046 may boost a discussion about where we want to go and how to get there.

BLOCKCHAINSNATCH:
A CHOOSE YOUR OWN ADVENTURE™ GIKII PAPER THAT *PROBABLY* DOESN’T INFRINGE CHOOSECO’S IP RIGHTS. OR NETFLIX’S. OR PROPOSE SOLVING ANYTHING WITH BLOCKCHAIN.

Adrian Aronsson-Storrier

In an effort to attract a $25 million trade mark infringement lawsuit[1] against the Gikii organisers, for this paper YOU are the star of the story! Choose Your Own (academic) Adventure™[2] with interactive branching video pathways and over 40[3] different endings! Do you want to hear a GIKII paper on the use of interactive video for legal education? Do you prefer to explore the limits of AI authorship and copyright with an academic paper written by a machine learning algorithm? Or are you hiking in Snake Canyon when you find yourself lost in the dimly lit Cave of Time? Whatever you do, don’t click on the secret, forbidden button to hear an interactive paper on blockchain and COVID-19 tracing applications…

BLOCKCHAIN IN-GAME COLLECTABLE ITEMS AND COPYRIGHT LAW: COPYRIGHT IMPLICATIONS OF A NEW WAY OF CREATIVE WORKS CONSUMPTION

Dr. Bianca Hanuz, University of Liverpool

Blockchain is the technology that supports cryptocurrency as it enables the decentralised transfer of value between anonymous parties on the internet. Blockchain generates an audit trail of all cryptocurrency transactions to prevent the double spending of crypto. In the last years, a large number of proposals are put forward whereby blockchain is set to innovate copyright. One area of blockchain use that witnesses promising developments is the online gaming market. In this context, blockchain technology is largely used to tokenise, i.e. link a value, which represents an in-game collectable item such as a sword, with an entry on the blockchain in such a way that the ‘ownership’ of that in-item or transfer of that ‘ownership’ from one user to another can always be accurately tracked and remunerated with reference to the blockchain. This new economy for in game items enables a number of facilities for developers and game players. For example, some game developers are using blockchain to introduce a degree of interoperability which enables users to multitask in-game items across various games blockchain games or games which support blockchain plug-inns. In this context, a player can use for example a sward he purchased in game A in game B. Other facilities are available for players of blockchain games such as the option to sell, trade or lend in game items to other users. Overall, players enjoy more flexibility over the use of in-game collectibles.

From a copyright perspective tokenised in-game items raise interesting questions. Who owns the copyright in a tokenised in-game collectable figurine? What is the scope of the licence that users receive? Under which copyright regime should in-game items be regulated? How do these new means

[1] Chooseco LLC v. Netflix, Inc., No. 2:19-cv-08 (D. Vt. Feb. 11, 2020).
[2] EU Trade Mark EU018134141 ‘CHOOSE YOUR OWN ADVENTURE, Holder: Chooseco LLC
[3] Not a guarantee.

of in game item consumption sit with the EU copyright framework? This presentation will analyse the relationship between blockchain supported in-game collectible items and copyright law to address these issues.

MISSING CRYPTOCURRENCY: IN SEARCH FOR CONSUMER PROTECTION IN THE MLM SPACE

Catalina Goanta, Constanta Rosca, Rūta Liepiņa, Bogdan Covrig

During the past decade, blockchain technology has been a volatile hype. Among others, the blockchain space has gained a lot of attention from opportunistic entrepreneurs who have seen this as an opportunity to open the door for cryptocurrency investments to many technologically illiterate consumers attracted by get-rich-fast business schemes.

The most well-known illustration of this problem is reflected by the OneCoin scandal, a world-wide scam thought to have cost consumers and investors a whopping total of 4 billion pounds. This scheme's success is strongly linked to the way in which the company operated. Instead of getting investments via initial coin offerings from angel investors, like all other tech companies creating new cryptocurrencies or virtual tokens, OneCoin gathered funds by adopting a multi-level marketing sale technique.

Multi-level marketing and its evil twin concept (pyramid schemes) have long been on the agendas of authorities and regulators because of the consumer protection issues they raise. While the first is in principle a lawful business model, the latter is an outlawed practice due to its harmful nature. Pyramid schemes promote high gains by promising their affiliated sellers commissions for bringing additional sellers into the schemes. New members/sellers buy into the scheme but end up losing their investments, as most often the products or services which are the object of the sale do not exist. In the case of OneCoin, this product was a fake cryptocurrency, sold alongside with 'educational materials' packages to new members. While authorities in countries such as China or the US started cracking down on OneCoin, the model of using MLM for cryptocurrency investments has inspired other businesses in this space, with former OneCoin investor Nils Grossberg launching DagCoin.

This paper takes the angle of consumer protection to ask the question of whether the current legal framework in the EU is adequate in protecting consumers against fake cryptocurrency commerce**.** The paper is structured as follows. The first part makes a brief overview of what exactly a cryptocurrency is and proposes criteria for the distinction of ‘fake’ cryptocurrencies in commercial communication. The second part looks at the history of MLMs to discern their core features, which are further compared to the features of a pyramid scheme in part three. This part also looks into European consumer protection instruments, namely the Unfair Commercial Practices Directive and the Misleading and Comparative Advertising Directive and discusses relevant case law of the CJEU on the blacklisted prohibition of pyramid schemes (Annex point 14 UCPD). Lastly, the paper suggests improvements for the current framework.