1:1

Reconciling the Material and Immaterial Dissemination Rights in the Light of the Developments under the EU Copyright Acquis

Liliia Oprysk, University of Tartu

Abstract:

Copyright protection ought to serve the public interest by incentivising artistic labour and facilitating dissemination of creative works. Inevitably, the grant of exclusive rights under copyright comes at the cost of reduced public access to protected works and distorted competition. Therefore, control conferred by exclusive rights is not absolute but must be confined to what is necessary to achieve the rationales of protection.

Development of technology has challenged the established approaches to defining the appropriate scope of exclusive rights. Not least, the emergence of the digital environment as a new dissemination channel has contested the traditional distinction between the rights of material and immaterial dissemination enshrined under the EU copyright *acquis*. Secondary EU law seemingly denies any general limit to the right holder's control over any primary or secondary acts of communication while exempting secondary distribution. The recent development under the CJEU jurisprudence, on the other hand, suggests that the variable circumstances of exploitation of a work call for a more nuanced approach.

The project explores the development of the key economic rights under the EU copyright *acquis* against technological advancements and the distinction drawn between material and immaterial dissemination rights under secondary EU law. It advances the idea that the assumption enshrined under the EU copyright framework at the very outset of harmonization is outdated and suggests reconciling of the approaches to regulating dissemination-related rights in the light of the developments under the *acquis*. To this end, a normative framework for evaluating the justifiability of extending the reach of exclusive rights beyond authorizing every initial dissemination of a work is offered. Unlike the current approach to the scope of exclusive control, the outlined criteria capture the changing circumstances of a work's exploitation and the diverse interests involved.

1:2

Law and Technological Change: A Typology

Mikko Huttunen, University of Lapland

Abstract:

The traditional system of air law has been primarily created for manned aircraft, that is, aircraft whose pilot is on board. In recent years, however, the proliferation of unmanned aircraft systems (UAS), or drones, has instigated a change in the system. Several characteristics of drones have led to problems of uncertainty as well as under- and over-inclusion: simply put, many pre-existing rules have turned out to be unfitting.

The responses to the issue by the International Civil Aviation Organization (ICAO) and the European Aviation Safety Agency (EASA), the two leading regulatory bodies of air law, have been diverse. In some cases, no regulatory action has been deemed necessary. For example, Article 8 of the Convention on International Civil Aviation (titled Pilotless Aircraft) has been viewed as applying directly to drones.

More often, however, an attempt has been made to either directly or indirectly apply pre-existing rules to drones. For instance, the ICAO has declared that rules of the air apply to international UAS operations. Meanwhile, EASA has adopted rules pursuant to which drones must be registered, but electronically as opposed to on paper. In some cases, it has been necessary to establish alternative institutions, such as the specific category of operations, with its own risk assessment. Finally, it has also been hinted that transforming the pre-existing rules of airspace management may be necessary in order to create a seamless airspace for all aircraft.

These observations have led me to a typology of the approaches the legislator may employ when faced with technological change: passivity, direct and indirect application, alternative rules, and transformation. While the typology is based on a single case study of the international and European regulation of drones, it might be generalized beyond the context of air law.

Abuses of Dominant ICT Companies in the Area of Data Protection

Aleksander Wiatrowski, University of Lapland

Abstract:

In my dissertation, I am focusing, among other issues, on dominant companies. I am not interested in actions of smaller, less significant, in economic and legal point of view, entities. Microsoft, Facebook, Google, etc., are so huge and influential that they are already known for abusing their position in numerous cases. Their economic, global position allows them to easily pay all the fines. So far it seems that tools countries and organizations all over the world have, are not enough to stop dominant companies from their illegal actions. I would like to explain why dominant companies are in very comfortable position, and why focusing on them is so important in understanding threats to privacy and data protection and data security, especially with the mass surveillance in background. I focus on dominant companies because the bigger power on the market has a subject the bigger abuser it can be. Companies selected by me, by the fact they are dominant, have a significant and major impact on legal and factual actions in a wide area of protecting and securing data as well as privacy.

2:1

Certification in Data Protection

Anna Maja Wallin, University of Copenhagen

Abstract:

Technological developments and the global economy have brought new challenges to data protection. To regulate the developments, the European legislator introduced self- and co-regulatory mechanisms, such as certifications. In IT-law the liability for certifications is determined on a contractual or tortious basis. In the GDPR, certifications serve different functions and allow for different benefits. However, it is uncertain whether self- and co-regulatory mechanisms can adequately meet the objectives of data protection. The project explores the interaction of self- and co-regulatory instruments and human rights. Is it tenable to certify GDPR compliance? How can compliance be measured and audited?

The purpose of the research is to bring clarity to the application of personal data protection to certifications, standards, and seals. The project combines an analysis of case law, guidance-papers, and literature. The project argues that while certifications support accountability, certifications do not necessarily ensure reflexivity to human rights discourse. In addition, a certification only provides a rebuttable presumption for compliance with a validity of three years. The project, therefore, argues that the costs and benefits are insufficiently balanced to make certifications attractive.

2:2

Liability and the Right to Compensation for Damage Caused by Unlawful Processing of Personal Data

Fredrik Sandberg, Stockholm University

Abstract:

The project is about the right to compensation and liability for damage caused by unlawful processing of personal data. How does liability and the right to receive compensation in these situations differ from what is generally the case in tort law? Do the situations where the protection of personal data come in to play call for other solutions than the ones generally provided by tort law? If that is the case, why is it so and what, more exactly, are the relevant reasons? Yet another important question is if the current legal situation lives up to and is suited for the needs the technological and societal developments entail? The general or overarching purpose of the project is to establish and explain the relevant legal conditions and reasons for compensation in the case of unlawful processing of personal data. In order to achieve that, the ambition is to present a coherent theory of compensation and liability in relation to data protection. The aim is to provide an understanding that facilitates legal certainty for data subjects and data controllers (and processors) as well as a continued critical discussion on legal developments.

2:3

Responsible Facial Recognition Technologies: Toward a Comparative Study of Regulation in the EU and China

Ruyi Ding, Stockholm University

Abstract:

Facial recognition technology (FRT) has taken a quantum leap in recent years, which is primarily due to advances in computer vision and artificial intelligence (AI). FRT has increasingly been incorporated into people's everyday lives. The rapidly developing technology is able to serve multiple purposes, including but not limited to physical and logical access control, security and surveillance, recreational and social networking, campus/workplace management, marketing and customer services, medical and healthcare services, etc. While FRT does benefit individuals and society at large in many ways, it might as well present significant risks (e.g., data protection risks, privacy risks, technological bias, etc.) from legal and ethical points of view. These risks are related to the nature itself of facial-recognition data, the architecture and specifications of a facial recognition system (FRS), and the practical real-world applications of FRT. Thus this project aims at discussing the legal and ethical boundaries of using FRT. The core research question is: What is meant by "responsible FRT", and how lawmakers and regulators in the EU and China respond to the risks posed by FRT for a responsible future? Several additional research questions are raised: What kinds of reasonable restrictions must be placed on the use of FRT? What are the impacts of GDPR on FRT? Does the EU need a legal framework, beyond GDPR and Law Enforcement Directive, to wisely regulate FRT? (If so, why?) What are the similarities and differences between the EU and China regulatory approaches to FRT?

2:4

Processing of Medical Personal Data for Research Purposes

Mikhail Zhuravlev, Higher School of Economics

Abstract:

Mikhail Zhuravlev is a junior research fellow at the International Laboratory for IT and IP Law of the National Research University Higher School of Economics. His PhD research devoted to the legal aspects of data sharing and data protection in eHealth. This presentation is focused on the legal grounds for processing of medical personal data for research purposes. Comparing the requirements of the Russian legislation on personal data and GDPR the research stresses the necessity for more flexible approach to processing of personal data for public purposes, including research and statistics. It suggests differentiation of consent models, specification of requirements for depersonalization and imposing additional demands on transparency and security on data controllers (data processors). The research argues that these kinds of measures can mitigate tensions between digital economy needs and barriers arising from data protection law through striking a flexible balance between public and private interests.