Stanford – Vienna
Transatlantic Technology Law Forum

A joint initiative of
Stanford Law School and the University of Vienna School of Law

Transatlantic Antitrust and IPR Developments

Bimonthly Newsletter

Issue No. 2/2022 (October 9, 2022)

Contributors:

Amedeo Rizzo, Christine Carter, Gabriel M. Lentner, Jan Czarnocki, Marie-Andrée Weiss, Martina Acciaro, Salome Kohler, Sebastian Pech

Editor-in-chief: Juha Vesala

Contents

About the contributors

Amedeo Rizzo is a D.Phil. in Law and Tutorial Fellow at the University of Oxford, UK, where he conducts research in taxation, innovation, and development. He is an Academic Fellow of Taxation at Bocconi University, Italy, and SDA Fellow of Tax and Accounting at SDA Bocconi School of Management, where he coordinates the Accounting & Tax Policy Observatory and the Transfer Pricing Forum. He is the director of the Innovation Policy Network and Research Fellow of the Working Party on Tax & Legal Matters. As a TTLF Fellow, his research focuses on the analysis of different types of tax incentives to enhance innovation through intellectual property and research and development activities.

Christine Carter is a research fellow with the Stanford-Vienna Transatlantic Technology Law Forum (TTLF) since August 2022. Her research interests lie in the areas of EU law, Law & Economics, and Employment law. Within these areas, she focuses on the regulatory, economic and technical implications of emerging technologies, particularly in relation to the regulation of Algorithmic Governance, Big Data, Digital Surveillance and Platform Economies. She holds both a BA (Double-First Class Honors) and a LLM (Distinction Honors) from the University of Cambridge, UK, where she has been awarded numerous academic prizes and studentships for her legal achievements. She has worked in the International Arbitration practice group of Arnold & Porter LLP in London where she assisted the practice group in various cases involving the representation of sovereign States and multi-national corporations in investor-state arbitrations and international commercial arbitrations. Previously, she has served as the Deputy Editor-in-Chief for Per Incuriam at the University of Cambridge, as well as the 2021 LLM College Representative on the Staff-Student Consultative Committee of the University of Cambridge. Additionally, she has delivered lectures on behalf of the Cambridge Law Faculty on the subject of Youth Justice for the 2021 LLM cohort. She also has served as a volunteer researcher for the AMICUS ALJ Campaign in London during Summer 2019.

Gabriel M. Lentner is an Assistant Professor of Law at the Danube University Krems and currently a Visiting Scholar at Harvard Law School. He holds a Ph.D. in International Law, a diploma with the highest distinction in European Studies from the University of Vienna (2010), and a diploma in Law & Logic from Harvard Law School and the European University Institute in Florence (2013). His main research interests are international investment law, EU law, and public international law. As a TTLF Fellow, his current research focuses on the protection of intellectual property rights through international investment agreements.

Jan Czarnocki is a Doctoral Researcher and Maria Skłodowska-Curie Fellow at the KU Leuven Centre for IT & IP Law, Belgium. He currently researches privacy and data protection, focusing on biometric and health data in the IoT-AI context within the Privacy Matters (PriMa) ITN project. His research encompasses the intersections of law, philosophy, technology, and

policy. Jan was appointed a TTLF Fellow in 2022. He is also an Affiliated Fellow at the Jagiellonian University Private Law of Data Project, Poland, and has been a Visiting Researcher at the Julius Maximillians University of Wurzburg Human-Computer Interaction Group, Germany. Before that, he was a trainee in the External Policies Directorate of the European People's Party Group in the European Parliament and a "European View" editor-intern at the Wilfried Martens Centre for European Studies. He holds a Master's degree in law from the University of Warsaw, Poland, and an LL.M. degree in Comparative Law from the China University of Political Science and Law in Beijing.

Marie-Andrée Weiss is an attorney admitted in New York and in Strasbourg, France. Before becoming an attorney, she worked for several years in the fashion and cosmetics industry in New York as a buyer and a director of sales and marketing. She graduated from the University of Strasbourg in France with an M.A. in Art History, a J.D. in Business Law, an LL.M. in Criminal Law, and an LL.M. in Multimedia Law. Marie-Andrée also graduated from the Benjamin N. Cardozo School of Law in New York City with an LL.M. in Intellectual Property Law. She is an attorney in New York and her solo practice focuses on intellectual property, privacy, data protection, and social media law. As a TTLF Fellow, Marie-Andrée's current field of research is a comparison of the powers given to users by the EU Digital Service Act and by the Facebook Oversight Board.

Martina Acciaro works as Research Assistant at SDA Bocconi Business School, Accounting and Tax Policy Observatory, for which she conducts research and support activities in international taxation, business taxation and transfer pricing. She helps with the coordination of the Transfer Pricing Forum, contributing to the seminars and workshops organized by the center. She is also a Research Associate of the Innovation Policy Network, in the area of Taxation & Law, carrying out policy-oriented research about taxation of the digital economy and new technologies.

Salome Kohler is a Research Assistant at the University of Zurich, Switzerland. In addition to her work at the Chair for Banking & Financial Market Law (Professor Kern Alexander), she is a doctoral candidate at the University of Zurich and works on online privacy in the American and European context. She was involved in a project conducted by UBS plc. and the University of Zurich on ESG investing and also worked as a Research Assistant at the University of St. Gallen, Switzerland. Salome graduated in law as well as in economics from the University of St. Gallen and the University of Bern in Switzerland. She earned an LL.M. degree at the University of California, Los Angeles (UCLA) and was awarded the Dean's Tuition Fellowship at UCLA School of Law. Salome has been a TTLF Fellow at Stanford Law School since 2022.

Sebastian Pech graduated in law from Ludwig Maximilian University of Munich, Germany, earned an LL.M. in IP/IT law at the Duke University School of Law, and a Dr. jur. (Ph.D. in law)

at the University of Bayreuth, Germany. His experience includes, among others, positions at the legal publishing house C.H.Beck, the Institute for Copyright and Media Law (IUM), and law firms specialized in IP and IT law. Sebastian's research focuses on the effects of digital transformation on the legal system, especially the challenges (and opportunities) for technology, copyright, and media law, from both the European and the US perspective. He also publishes regularly on these topics. He is a member of the German-American Lawyers' Association (DAJV), the German Association for the Protection of Intellectual Property (GRUR), and the Copyright Society of the USA (CSUSA). Sebastian has been a TTLF Fellow since 2021.

Antitrust
European Union

The Digital Markets Act: EU's Big Policy Promise for Big Tech

By Christine Carter

The EU Digital Market Act (DMA) is the latest piece of the European Commission's digital reform agenda to create a comprehensive and sophisticated regulatory regime for the Big Tech industry. The DMA was originally proposed in December 2020 and has recently passed a final vote with an overwhelming majority in the European Parliament on the 5th of July 2022 with 588 votes in favor and 11 against the act. The act is expected to be formally adopted by the European Council in October 2022. Following such, big tech companies who are subject to the jurisdiction of the act will have to notify the European Commission within a period of 2 months, starting from Spring 2023, as well as then act in compliance with the DMA's new regulatory obligations by early 2024. In doing so, the DMA contributes to Europe's digital reform agenda of *"making Europe fit for the Digital Age"* and will come into force alongside the EU Digital Services Act (DSA)[1].

Background

The DMA is introduced to deal with the rapid proliferation of the digital economy over the last decade which has resulted from the vast growth of big tech companies. The digital economy is specifically characterized by the technological control of the so-called "GAFA" sector (Google, Amazon, Facebook and Apple). In response to their increased market share in the EU, there has been a series of legislative challenges and investigations that have been litigated in front of both national and EU courts. One of the most seminal of these legal disputes arose in the investigation of the European Commission[2] against Google in what has become to be known as the *Google Shopping* case. Consequently, concerns have arisen that European Courts are particularly slow to deal with competition law issues arising from the digital market and lag behind the speed in which the digital economy is evolving.

Legislative Objective

Against this background, the European Commission introduced the DMA as a

[1] European Commission (2022), Shaping Europe's Digital Future https://ec.europa.eu/info/sites/default/files/communication-shaping-europes-digital-future-feb2020_en_4.pdf

[2] EU Commission, Press release of Nov 30, 2010, *Antitrust: Commission probes allegations of antitrust violations by Google*

series of *ex ante* obligations that can react quickly and meaningfully to the legal challenges raised by the Big Tech industry. The DMA takes an unprecedented step in shifting from a largely self-regulated to a regulated model of law enforcement in the Big Tech industry. Margrethe Vestager, Vice President of European Commission described the act as a "*global movement*" that will "i*nspire all over the planet*"[3]. The DMA implements the policy agenda in a series of regulatory obligations for large tech corporations and provides the European Commission with a new set of enforcement powers to take action where those obligations are not met by Big Tech. This regulatory approach seeks to address the current short comings of EU competition law in regulating the digital market and ensuring an equal-level playing field among large tech corporations.

Gatekeepers and Core Platforms Services

To fall within the act's definition of a gatekeeper, a company must provide one or more of the *core platform services* defined in Article 2(2) of the DMA and meet a series of qualitative and quantitative criteria which are listed in Article 3(1).

- A company must have a significant impact on the market: this is presumed where companies have an annual turnover of € 7.5 billion within the European Economic Area (EEA) or a worldwide market valuation of € 75 billion and it provides the same core platform service in at least three Member States (Articles 3(1)(a) and 3(2)(a));

- A company must operate one or more important gateways to customers: this is presumed where companies have at least 45 million monthly individual end-users or 100,000 business users located in the EU in the last financial year (Articles 3(1)(b) and 3(2)(b);

- A company possesses an entrenched and durable position: this is presumed to be met if the meets the above two criteria) in each of the last 3 financial years (Articles 3(1)(c) and 3(2)(c))

Companies that do not meet the quantitative criteria may still be designated as gatekeepers on the basis of a qualitative assessment carried out by the European Commission pursuant to Article 4. Companies that fall within the definition of gatekeepers must comply with the obligations laid out in Articles 5 - 7 and 14 of the DMA. These obligations are roughly split into the following themes: obligations of data protection, device neutrality, transparency in online advertising, ranking neutrality, neutrality towards intermediaries and distributers, and enforcement obligations. The obligations are divided into two different levels of severity. The first type are *black list* obligations which are directly applicable to gatekeepers without further details. The others are *grey list*

[3] European Parliament, Press Release March 24, 2022, *Deal on Digital Markets Act: EU rules to ensure fair competition and more choice for users*

obligations that contain obligations that may be specified in further detail by the Commission following a dialogue with the gatekeeper.

Black List Obligations

These include; prohibiting gatekeepers from processing, combining, signing or cross-using personal data without users' consent (Article 5(2)), prohibiting gatekeepers from preventing business users from offering products or services through other channels (Article 5(3)), prohibiting anti-steering provisions (Articles 5(4)-(5)), prohibiting restrictions on businesses from raising issues with authorities (Article 5(6)), prohibiting gatekeepers from requiring users to use gatekeepers' identification or payment services in third party apps or web browsers (Article 5(7)), prohibiting gatekeepers from bundling subscriptions or registrations (Article 5(8)), requiring gatekeepers' disclosure of advertisements, prices, revenue share information (Articles 5(9)-(10)).

Grey List Obligations

These include prohibiting gatekeepers' use of users' data that is not publicly available to compete with business users (Article 6(2)), requiring gatekeepers to allow app uninstallation, changing defaults and choice screens and, allow the installation of third party apps and app stores on their operating systems (Article 6((3)-(4)), prohibiting gatekeepers from deploying of discriminatory rankings against third party services and products (Article 6(5)), prohibiting restrictions on multi-homing (Article 6(6)), requiring interoperability of operating systems and virtual assistants (Article 6(7)), requiring the provision of access to performance measuring tools (Article 6(8)), requiring data portability (Article 6(10)), requiring search data sharing (Article 6(11), requiring fair access to app stores, search engines and social networking services (Article 6(12)), preventing restrictions on the termination of end-users' use (Article 6(13)), requiring interoperability for messaging services (Article 7).

Notification of Mergers

The DMA also imposes a duty on gatekeepers to inform the European Commission about planned mergers with other platform services or digital entities under Article 14 of the act. This provision will apply to gatekeepers regardless of whether they are subject to merger controls at either national or international law and is designed to keep the European Commission informed about their market share and aware of any potential killer acquisitions that would create barriers to the entry of the internal market. The DMA therefore allows the European Commission to deal with these issues preemptively without requiring the threshold of Article 22 of the EU Merger Regulation to be met. In so doing, the DMA considerably strengthens the merger control regime of the EU.

Enforcement

The DMA gives the European Commission several enforcement powers in the event of a gatekeeper's non-compliance with the aforementioned obligations. The European Commission may impose a fine of up to 10% of the gatekeeper's worldwide turnover from the previous financial year (or in the case of less serious infringements up to 1%) or additionally may impose a further fine of up to 20% of a gatekeeper's worldwide turnover from the previous financial year in the event of a repeated violation under Article 30 of the DMA. The imposition of periodic penalty payments is also permitted under Article 31 of the DMA. In the event of systematic non-compliance, the European Commission may also open up an investigation against the gatekeeper. In addition to these sanctions granted to the European Commission, it is expected that individuals may also take private actions against gatekeepers in front of national courts under Article 39 and 42 of the DMA.

Taxonomy within the EU Legal Order

Recital 10 of the DMA explains that the act is without prejudice to Articles 101 and 102 of the TFEU and therefore will operate in parallel to the existing body of EU Competition law and relevant EU Merger Control laws. The hierarchy between the DMA and national member state laws will depend on whether the national law is a *regulatory* or a *competition law*. Where the national measure is a *regulatory law*, the DMA will have the effect of superseding such pursuant to Article 1(5) of the DMA. Where the national measure is a *competition law*, the DMA does not supersede such subject to the exception in Article 1(6) that applies to national laws that are applied to undertakings other than gatekeepers or amount to the imposition of further obligations on gatekeepers.

Conclusion

The DMA certainly brings a lot of legislative promise to the table, which has been met with a great deal of hope in the legal world. The act itself is extremely detailed and concise and leaves little room for ambiguity. The act also creates a hierarchy between *Black* and *Grey list* obligations to enable the European Commission to deal with the former in a manner that is rather strict and with the latter in a manner that is more conducive to further collaboration and cooperation in the resolution of these legal requirements. From this perspective, the DMA symbolizes a fair compromise between the need to protect digital rights and competition interests in a technological world, as well as the need to recognize the political, social and economic reality in which these rights operate, and the ability to strike economic and political compromise where necessary to reach consensus. This is achieved in a manner that is efficient and innovative, which will hopefully provide certainty and clarity on the regulatory status of many Big Tech companies in Europe and avoid elongated legal

proceedings in front of national and supranational courts and tribunals in cases of dispute. However, what will remain left to be seen is how effective the act will be on emerging gatekeepers and companies that do not meet the Article 3 requirements. This will be subject to the intensity of the impact assessment review of the European Commission and it will be extremely interesting to see how the EU will go about in exercising its regulatory mandate to subject companies to the DMA.

Intellectual Property
United States

"Royale with Cheese" – Copyright Issues Related to NFTs in Miramax v. Tarantino

By Sebastian Pech

Recently, non-fungible tokens (NFTs) have received a lot of attention owing to some spectacular digital art sales. Thereupon, several artists have started selling their work in the form of NFTs, including the award-winning filmmaker *Quentin Tarantino*, who was later sued by the film production company *Miramax*. This contribution analyses the copyright issues surrounding NFTs that emerge from the lawsuit.

I. Details of the Lawsuit

In November 2021, *Quentin Tarantino,* in collaboration with *Scrt Labs,* announced that he would auction off seven different parts of the handwritten screenplay of the 1994 blockbuster *Pulp Fiction* in the form of NFTs.[4] The so called "Private NFTs" provide their owners with specific privacy features, especially "content viewable only by the owner of the NFT".[5]

Shortly after the announcement of the *Tarantino NFT Collection*, *Miramax* sued *Tarantino* in the *Central District of California* for breach of contract, copyright infringement, trademark infringement, and unfair competition.[6]

In 1993, *Tarantino* had granted *Miramax* "all rights (including all copyrights and trademarks) in and to [Pulp Fiction] (and all elements thereof in all stages of development and production) now or hereafter known".[7] However, *Tarantino* expressly reserved some rights, namely the "soundtrack album, music publishing, live performance, print publication (including without limitation screenplay publication, 'making of' books, comic books and novelization, in audio and electronic formats as well, as applicable), interactive media, theatrical and television sequel and remake rights, and television series and spinoff rights".[8]

Miramax argues that selling parts of the screenplay in the form of NFTs violates its

[4] *Quentin Tarantino Revealed as Iconic Artist Behind First-Ever Secret NFTs*, *Showcasing Never-Before-Seen Work Revealed Only to NFT Owner*, GLOBE NEWSWIRE (Nov. 2, 2021), https://www.globenewswire.com/news-release/2021/11/02/2325448/0/en/Quentin-Tarantino-Revealed-as-Iconic-Artist-Behind-First-Ever-Secret-NFTs-Showcasing-Never-Before-Seen-Work-Revealed-Only-to-NFT-Owner.html.
[5] *Id.*
[6] Miramax, LLC v. Tarantino, 2:21-cv-08979-FMO-JC (C.D. Cal. 2021).
[7] Complaint at 24, Miramax, LLC v. Tarantino, 2:21-cv-08979-FMO-JC (C.D. Cal. 2021).
[8] *Id.*

right to create derivate works set forth in § 106(2) Copyright Act.[9] *Tarantino*, on the other hand, claims that he did not grant *Miramax* any rights to the screenplay[10] and even if this should be the case, he was acting within his reserved rights, especially the right to print publication.[11]

In January 2022, the first NFT based on a scene where the movie's protagonists *Jules* and *Vincent* are talking about life in Europe and in particular the French term for a "quarter pounder with cheese" ("royale with cheese") was sold for $1.1 Million.[12]

Only a few days later, the sale of the other six scenes was indefinitely postponed due to "extreme market volatility".[13] This gave rise to speculations ranging from fear of the pending litigation and insufficient demand from buyers to technical problems.[14]

In September 2022, the lawsuit ended by a surprising settlement between *Miramax* and *Tarantino*,[15] shortly after the parties had informed the court that previous negotiations had failed.[16]

II. NFTs in a Nutshell

Tokens are digital representations of assets on the blockchain. A blockchain is a highly tamper-resistant and transparent database. The term "token" is often used as a synonym for cryptocurrency, but a token can represent any form of economic value, such as commodities, real estate, company shares, or copyright protected works. Tokens can be bought and sold using blockchain-based "smart contracts," which are computer programs that execute transactions and enforce contractual terms automatically.

Fungible and non-fungible tokens are distinct from each other. Fungible tokens are interchangeable with other tokens. Cryptocurrencies, such as Bitcoin, are examples of fungible tokens. Every unit of Bitcoin is equivalent to another and has the same

[9] *Id.* at 17.
[10] Notice of Motion and Motion for Judgement on the Pleadings at 14, Miramax, LLC v. Tarantino, 2:21-cv-08979-FMO-JC (C.D. Cal. 2021).
[11] *Id.* at 17.
[12] *SCRT Labs Announces Triumphant Sale of First Never-Before-Seen-Or-Heard Tarantino NFT for $1.1 Million*, BUSINESS WIRE (Jan. 24, 2022), https://www.businesswire.com/news/home/20220121005513/en/SCRT-Labs-Announces-Triumphant-Sale-of-First-Never-Before-Seen-Or-Heard-Tarantino-NFT-for-1.1-Million.
[13] @LegendaoNFT, TWITTER (Jan. 28, 2022, 9:59 PM), https://twitter.com/LegendaoNFT/status/1487168591556456448.
[14] Eduardo Próspero, *What Happened To Tarantino 's "Pulp Fiction" NFT Collection? The Strange Finale*, NEWSBTC, https://www.newsbtc.com/crypto/what-happened-to-tarantino-s-pulp-fiction-nft-collection-the-strange-finale/ (last visited Sept. 9, 2022).
[15] Notice of Settlement at 1, Miramax, LLC v. Tarantino, 2:21-cv-08979-FMO-JC (C.D. Cal. 2021).
[16] Edvard Pettersson, *Tarantino, Miramax settle lawsuit over 'Pulp Fiction' screenplay NFTs*, COURTHOUSE NEWS SERVICE (Sept. 8, 2022), https://www.courthousenews.com/tarantino-miramax-settle-lawsuit-over-pulp-fiction-screenplay-nfts/.

value. By contrast, a non-fungible token (NFT) is unique and thus not replaceable by other tokens.

Due to this feature, NFTs are used to represent unique assets on the blockchain, especially (digital) art or, in the present case, parts of a screenplay. Associating assets with an NFT allows authors, collectors, and owners to document and verify the provenance of the asset in question. In summary, an NFT can be best described as a forgery-proof certificate that confirms the ownership of a specific asset and/or the rights with respect to the said asset.

III. Analysis of the Copyright Issues Related to NFTs

Creating (or "minting") an NFT for a copyright protected work does not, in most cases, lead to a reproduction of the work in the sense of § 106(1) Copyright Act. A reproduction requires a copy of the work which is defined under § 101 Copyright Act as a "material object[…] in which a work is fixed by any method now known or later developed, and from which the work can be perceived, reproduced, or otherwise communicated, either directly or with the aid of a machine or device".[17] Since storing information on a blockchain is very expensive, in most cases no copy of the work itself, but only its digital representation is saved on the blockchain, comprising data identifying the underlying work, specifically a hyperlink pointing to a file stored somewhere on the web.

In the case of the *Tarantino NFT Collection*, it is not entirely clear whether the digital version of the screenplay is saved on the blockchain or "off-chain". The definition of a "Secret NFT" in the terms and conditions for the sale as "a Non-Fungible Token minted on the Secret blockchain network containing a digital file of a Publication"[18] indicates that it is indeed stored on the blockchain. However, *Scrt Labs'* description of a "Secret NFT" on its website only mentions metadata and links to files, not works themselves stored on the blockchain.[19] Due to the high costs associated with saving high-resolution scans on the blockchain, storage "off-chain" is far more likely.

The right to prepare derivative works based upon the copyrighted work (§ 106(2) Copyright Act) is not infringed either. A derivative work has to "contain[…] a substantial amount of material" from the preexisting work,[20] as it is the case with "translation, musical arrangement, dramatization, fictionalization, motion picture version, sound recording, art reproduction, abridgment, condensation, or any other form in which a work may be recast, transformed, or adapted".[21]

[17] 17 USC § 101.
[18] *Secret NFT Purchase and License Agreement,* TARANTINO NFTS, https://tarantinon-fts.com/terms (last visited Sept. 14, 2022).
[19] *See Secret NFTs*, SECRET NETWORK, https://scrt.network/about/secret-nfts (last visited Sept. 14, 2022).
[20] Twin Peaks Prods. v. Publ'ns Int'l, Ltd., 996 F.2d 1366, 1373 (2d Cir. 1993).
[21] 17 USC § 101.

Metadata which contains information about a work, such as a hyperlink, cannot be considered a substantive part of that work.

Furthermore, the distribution right set forth in § 106(3) Copyright Act is also not violated, because the sale of the NFT does not affect the work as such, but only its representation on the blockchain. In *Perfect 10 v. Amazon*, the *Ninth Circuit* held that posting a hyperlink to a work on the Internet is not distribution of the work because the person who provides the link just enables others to access the work but does not "own" the work by hosting it on his server.[22]

Therefore, in the Copyright Act, there is no exclusive right of the copyright owner to create an NFT. This is a reasonable result since an NFT serves as a certificate of ownership of the underlying asset. No one would suggest that creating an equivalent certificate for traditional art, such as an oil painting or a marble sculpture, could constitute a copyright infringement.

As a result, for minting an NFT, it is irrelevant whether *Tarantino* assigned the rights to the screenplay to *Miramax* or whether an NFT creation for the screenplay is covered by *Tarantino's* reserved rights, for example the right to publication.

Conversely, making scans of the screenplay and storing them on a server is a reproduction in the sense of § 106(1) Copyright Act. In addition, selling these scans to the public constitutes distribution in the sense of § 106(3) Copyright Act. In dealing with these actions, it is indeed relevant whether *Tarantino* kept the rights to the screenplay, or at least the publication rights. However, this has nothing to do with NFTs; rather, it is a question of interpreting the contract between *Miramax* and *Tarantino*.

[22] *See* Perfect 10, Inc. v. Amazon.Com, Inc., 508 F.3d 1146, 1162 (9th Cir. 2007).

IV. Conclusion

From a legal perspective, the lawsuit's crux revolves around the question of how the contract between *Tarantino* and *Miramax* is to be interpreted, and not the fact that the screenplay was sold in the form of an NFT. However, since the lawsuit ended in a settlement, it will be unknow whether the court would nevertheless have made any comments on the copyright issues with respect to NFTs discussed here.

Intellectual Property
United States

What Would Lady Whistledown Say? Prince, Warhol and the Duke (of Hasting)

By Marie-Andrée Weiss

Fair use is a statutory exception to copyright infringement. The Copyright Act, 17 U.S.C. § 107, identifies four factors which may be considered by the courts when determining whether an unauthorized use of a work protected by copyright was fair: (1) the purpose and character of the use; (2) the nature of the copyrighted work; (3) the substantiality of the portion used in relation to the copyrighted work as a whole; and (4) the effect on the potential market for or value of the copyrighted work.

The first factor, the purpose and character of the use, has been interpreted in 1994 by the Supreme Court of the United States (SCOTUS), in *Campbell v. Acuff-Rose Music, Inc*., as requiring that the use is transformative, meaning that the new work "adds something new, with a further purpose or different character, altering the first with new expression, meaning, or message" (Campbell, at 579).

SCOTUS revisited its fair use doctrine last year, holding in *Google v. Oracle* that Google's copying of the Java SE AP was a fair use of that material as a matter of law, finding Google's use to be "transformative" as it sought "to expand the use and usefulness of Android-based smartphones […] offer[ing] programmers a highly creative and innovative tool for a smartphone environment" and being as such a use "consistent with that creative "progress" that is the basic constitutional objective of copyright itself", citing Feist Publications, Inc. v. Rural Telephone Service Co., at 349-350:

"The primary objective of copyright is not to reward the labor of authors, but `[t]o promote the Progress of Science and useful Arts'".

Indeed, Article I, Section 8, Clause 8, of the United States Constitution grants Congress the power "To promote the progress of science and useful arts, by securing for limited times to authors and inventors the exclusive right to their respective writings and discoveries."

Now SCOTUS has an opportunity to rule further on what use is transformative and thus, as an upcoming case is likely to influence fair use case law in the upcoming years.

Fair use and Prince: the Andy Warhol case

The Southern District Court of New York (SDNY) found in 2019 that the Prince Series created by Andy Warhol from a photograph

of musical artist Prince, taken in 1981 by professional photographer Lynn Goldsmith, was transformative.

Goldsmith's agency had licensed the photograph to Vanity Fair magazine in 1984 to be used as an artist reference to create an illustration. This artist was Andy Warhol, who created not only the illustration commissioned for the magazine, but also fifteen additional works, the sixteen works series now known as the Prince Series.

Goldsmith was not aware of the Prince Series, only learning about it after Prince's death in 2016, when Vanity Fair published on the cover of its tribute issue to Prince a work from the Prince Series different from the one originally commissioned by Vanity Fair. The work had been licensed to Vanity Fair by the Andy Warhol Foundation for the Visual Arts (AWF), which owns the copyright in the Prince Series.

AWF sued Goldsmith for a declaratory judgment of non-infringement. The Southern District Court of New York granted summary judgment to AWF, finding that the Prince Series was transformative, noting that that photograph taken by Goldsmith portrayed Prince as "not a comfortable person" and a "vulnerable human being," while Warhol's Prince Series portrayed him as an "iconic, larger-than-life figure."

The United States Court of Appeals for the Second Circuit, held, however, that the use was not transformative. AWF successfully petitioned to have the case heard by SCOTUS, which will hear next month the *Andy Warhol Foundation for the Visual Arts, Inc., v. Lynn Goldsmith* case, answering petitioner's question:

Is a work of art "transformative" when it conveys a different meaning or message from its source material, a view taken by the U.S. Court of Appeals for the Ninth Circuit, or should a court be forbidden to consider the meaning of the derivative work where it "recognizably deriv[es] from" its source material, as held by the Second Circuit Court of Appeals?

Fair use and the Duke (of Hastings): the Unofficial Bridgerton Musical case

AWF noted in its petition that it is the legality of the Prince Series which is the issue of the case. Fair use is the somewhat elusive concept allowing thousands of new works to be created each year, including many works created by "fans".

Abigail Barlow and Emily Bear ("Barlow & Bear") are fans of the Netflix series Bridgerton. They are also Grammy® award winners for their work, the Unofficial Bridgerton Musical. The work, first developed in real time on the social media platform *TikTok* on the premise "but what if Bridgerton was a musical?" found viral fame online, leading to a full album which won the 2021 Grammy® for Best Musical Theater Album.

Barlow & Bear performed their work on July, 28 2022 at the Kennedy Center in Washington D.C. in front of a sold-our audience. This concert appeared to have been the

proverbial last drop for Netflix, which filed a copyright infringement suit against the two musicians two days later, in the United States District Court for the District of Washington. Barlow & Bear were set to play at the Royal Albert Hall in London on September 20, 2022, but the show has been cancelled.

Netflix does not view these endeavors as fan fiction but argues that the Unofficial Bridgerton Musical "stretches "fan fiction" well past its breaking point. It is blatant infringement of intellectual property rights." Netflix alleges that some of the lyrics copy "verbatim" the dialogue of the show, for instance, in the opening number "*Tis the Season*," which allegedly copies the opening scene of the first episode of the series, using the character, the setting (Grosvenor Square, London, in 1813), "while also incorporating substantial dialogue verbatim. For instance, both works include the following dialogue regarding the setting and plot, spoken by Lady Whistledown: "Grosvenor Square, 1813. Dearest reader, the time has come to place our bets for the upcoming social season. Consider the household of the Baron Featherington."

Netflix further argues that Netflix has exclusive right to authorize derivative works based on the series. While the Bridgerton actors are dressed in costumes fit for characters living in 1813 London, the show features contemporary music played by classical musicians, such as Ariana Grande's *thank u, next*, played by the Vitamin String Quartet. Netflix may have plans to create its own Bridgerton musical, and the quality of the Unofficial Bridgerton Musical may well have a significant effect on the potential market or value of an official Bridgeton musical, the fourth fair use factor.

This case reflects the tension created by copyright between the need to "reward the labor of authors" as an incentive to create more works, which in turn benefits the public while "promot[ing] the Progress of Science and useful Arts" and the need for an exception to copyright, allowing some derivative works to be fair, even if using original works without permission, which also benefit the public and "promotes the Progress of Science and useful Arts"

There is no doubt that Barlow & Bear's music is creative, delights many members of the public, and that the two musicians have likely a long and successful career ahead of them (their latest creation is *Mexican Pizza The Musical*, created for Taco Bell and featuring… Dolly Parton.)

The Unofficial Bridgerton Musical is hardly the only "TikTok musical" and is not even the only TikTok musical to have gained fame outside of the social media platform. Ratatouille the Musical is a work created collaboratively with multiple TikTok users during the first phase of the pandemic, which was then presented online as a way to raise money for *The Actor Fund*, at the time where the closure of theaters prevented actors to make a living. The musical is a derivative work of the Walt Disney Ratatouille movie, but no legal threat was made against it.

The defendants in Unofficial Bridgerton Musical have not filed an answer. If the parties do not settle, the ultimate outcome of the case is likely to be influenced by the 2023 SCOTUS decision in the Andy Warhol Foundation for the Visual Arts, Inc., v. Lynn Goldsmith case and a possible new "transformative use as fair use" test.

Will Prince help the Duke?

Other Developments

United States

Can the Current Draft of the American Data Privacy and Protection Act (ADPPA) Be a New Hope for U.S. Federal Data Privacy Law?

By Salome Kohler

1. Some key provisions

In the U.S., there are once again attempts to improve privacy protection through a federal privacy act. Since it is still a draft, it is nevertheless worth mentioning the direction in which the main provisions of the act[23] are heading. The bill addresses concepts as the issue of data minimization, privacy by design, the right to consent and object, transparency, third-party collecting entities, the protection of sensitive data and vulnerable persons as children.[24] Privacy advocates say that the draft is still not strict enough to provide real privacy protection.[25] However, the bill provides substantial improvements to privacy as it intentions to reduce data collection by businesses to necessary issues and thus places a strong focus on data minimization, which is familiar from the approach of the European General Data Protection Regulation (GDPR).[26] The bill would also, among others, ban targeting ads to children and targeting based on sensitive data such as health data.[27]

2. Possible disadvantages

Critics fear, however, that a major goal of this comprehensive privacy bill is to limit future attempts to strengthen privacy protections by putting forward a federal law that would override state privacy laws ('preemption').[28] Unfortunately, such a provision is also included in the current draft, which could stop progressive states in their tracks toward strong privacy laws - much better would be a federal standard that allows for stronger state laws.[29]

---

[23] American Data Privacy and Protection Act (H.R. 8152), https://docs.house.gov/meetings/IF/IF00/20220720/115041/BILLS-117-8152-P000034-Amdt-1.pdf

[24] *Id.*

[25] H. Tsukayama, A. Schwartz, I. McKinney, L. Tien, *Americans Deserve More Than The Current American Data Privacy Protection Act*, EFF (Jul 24, 2022), https://www.eff.org/de/deeplinks/2022/07/americans-deserve-more-current-american-data-privacy-protection-act

[26] G. Edelman, *Don't Look Now, but Congress Might Pass an Actually Good Privacy Bill,* WIRED (Jul. 21, 2022), https://www.wired.com/story/american-data-privacy-protection-act-adppa/

[27] *Id.*

[28] *Id.*

[29] *Id.*

A federal privacy law that sets U.S. privacy regulation at a rather low standard would also increase legal differences with the internationally significant European General Data Protection Regulation (GDPR), making it more difficult to do business internationally.

3. Expected advantages

However, while a reduction in the strength of state laws is regrettable for consumers, it is welcomed by businesses, which could benefit from the legal certainty and simplification of the current legal situation and thus reduce the barriers to doing business caused by a multiplicity of privacy protection laws.[30]

Moreover, this would be a convenient solution for states that do not intend to enact privacy legislation but still want to benefit from a certain standard of privacy protection.

In addition, a comprehensive federal privacy law will ensure that the United States can play a leading role in setting the legal regime for privacy around the world.[31]

4. Conclusion

The appropriate level of privacy protection is still a point of contention, but the technological characteristics of data as such require a strong and protective federal law; a global legal approach would be even better.[32] A new federal law should be flexible and provide a good standard of protection for future and potentially broader threats to the right to privacy.

[30] L. Porter, B. E. Justice, *Federal Privacy Legislation – Is it finally happening?,* THE NAT. L. REV. (Jul. 26, 2022), https://www.natlawreview.com/article/federal-privacy-legislation-it-finally-happening

[31] *Id.*

[32] European Commission, *Proposal for a Regulation of the European Parliament and of the Council Laying down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending certain Union Legislative Acts, COM(2021) 206 final, 6, 18 (*2021).

Other Developments

European Union

Inferred Sensitive Data in the ECJ OT v Vyriausiojl. Is Everything Sensitive Data?

By Jan Czarnocki

On the 1st of August 2022, the European Court of Justice (ECJ) ruled on the interpretation of Articles 6.1 subparagraph e and 9.1 regarding processing personal data necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, and processing of special or sensitive categories of data.

The Regional Administrative Court in Vilnius, Lithuania asked the ECJ whether, among others, in view of Article 9(1) GDPR, which protects sensitive data, the Lithuanian law on reconciliation of interests obliges public officials to disclose their sensitive data publicly, can be reconciled with Art. 7 and Art 8 of the Charter of the Fundamental Rights of the EU. Thus, the question is whether in view of the GDPR, it is lawful to require public officials to disclose sensitive data on the publicly accessible website, including data based on which sensitive data can be inferred, such as the name and surname of the spouses and history of financial transactions. The answer to the question necessitated clarification of what should be considered sensitive data.

Narrow v broad interpretation of sensitive data

According to Art. 9 GDPR, sensitive data are data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data to uniquely identify a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

The ECJ stated that the obligation from the law on reconciliation constitutes a serious infringement on the right to privacy and data protection since mandatory disclosure of sensitive data is not proportional to the goal of fighting corruption. In the context of sensitive data disclosure, public interest in fighting corruption does not override the right to privacy and data protection, as well as a prohibition to process sensitive data from Art. 9 GDPR.

There would be perhaps nothing special in this case for data protection law doctrine if not for the reasoning provided by the ECJ, giving a broad interpretation of what is sensitive data. So far, there has been a lot of ambiguity regarding the precise scope of the Art. 9. It was unclear whether the provision should be interpreted narrowly, encompassing only data that directly reveals

information classified as sensitive, or whether it matters what can be inferred based on subject data.

According to the ECJ, the goal of the GDPR is to give a high level of privacy and data protection. Therefore, there is a need to understand the notion of sensitive data as also encompassing what can be inferred from the data disclosed, not only data at their "face value".

The ECJ argues that in view of the law on reconciliation of interests, if the public official is obliged to publicly disclose e.g., name and surname of his or her spouse, or financial transactions, from such data, further information can be inferred, including sensitive information.

It is the first time the ECJ explicitly endorsed a broad interpretation of sensitive data, finally clarifying years-long ambiguity regarding the precise scope of the Art. 9. There is no doubt now that narrow interpretation is not endorsed and that sensitive data is not only data immediately and directly disclosing traits enumerated in the Art. 9.

A challenge for tech giants

Although the case is not concerned with automated data processing, the ruling may have serious global consequences for personal data processing. Given the increasing capacities of AI systems to collect and infer knowledge, it is becoming more and more difficult to delineate between merely personal and sensitive data. Until now, data controllers and processors, such as Google or Facebook, could have argued that they do not process sensitive data since sensitive information is not disclosed immediately.

But from now on, it may turn out that most of the data processed by the tech giants are sensitive since, given their software's computing and analytics capacity, sensitive knowledge about individuals can be inferred. Thus, if after the ECJ ruling the data protection authorities and courts will adopt the Luxembourg court's line of reasoning—a likely outcome given that the ECJ is the highest instance interpreting the European Union law—then it means that for the processors and controllers with sophisticated enough analytical tools majority of personal data processed is sensitive data. That, in turn, would mean that the processing of such data is prohibited unless explicit consent is obtained.

This is a challenge because it is hard to obtain explicitly, informed, and valid consent for specified purposes in an online environment without an accusation of creating boilerplate contracts which people cannot understand. But on the other hand, the black box nature of AI systems also poses a legal risk since organizations may not even know whether their software can infer sensitive data, and what sensitive data, and based on what data. As a result, organizations will have to start to be much more self-conscious regarding their technical and organizational capacity to infer sensitive knowledge about people and how to manage this risk.

The more general conclusion from the ruling is that with it, and with more and more court and data protection authorities' decisions, the scope of ambiguity regarding the GDPR interpretation narrows. Therefore, for proper compliance with the data protection law, it will be increasingly harder to apply creative arguments and paperwork by lawyers to justify the processing without actually complying with the substance of the law. It means a much narrower permitted scope of personal data processing and perhaps even a need to reinvent business models based on revenues from personal data processing, such as those based on targeted ads.

Other Developments
European Union

Turning Point in intra-EU Investment Arbitration: *Green Power* and Other Developments

By Gabriel M. Lentner

For the first time, an international investment tribunal has rejected in *Green Power* jurisdiction on the basis of existing case law of the Court of Justice of the European Union (CJEU). These and other developments before courts in EU Member States appear to be the final nails in the coffin of intra-EU investment arbitration.

The Decision

The claim at issue was brought by two Danish companies under the Energy Charter Treaty (ECT) against alleged violations of investment protection thereunder against Spain in 2016. When the CJEU delivered its bombshell judgment in *Achmea*, where it held that intra-EU investment arbitration clauses in bilateral investment treaties (BITs) are incompatible with EU law, the tribunal in Green Power, bifurcated the proceedings.

Finding that there was no agreement of the parties regarding the law applicable to the question of jurisdiction, the arbitral tribunal decided that it had to examine this *ex officio* within the scope of its competence. In the view of the tribunal it was not only Art 26 ECT but other provisions as well as treaty and customary international law that needed to be taken into account. Then, disagreeing with an array of ICSID arbitral tribunals that took a different view, the tribunal argued that there was "a significant difference" between arbitrations under the SCC Rules and those under the ICSID Convention. This is because of the seat of an SCC arbitration being in the territory of an EU member state, unlike the ICSID system without such a seat. Through this the lex loci arbitri includes EU law which forms part of it. Ultimately, the arbitrators concluded that "the relevance and application of EU law to certain questions arising in these proceedings is inescapable, regardless of whether such law is characterized as part of international law or as part of domestic law".

What then followed was a lengthy discussion of the interpretation of Art 26(3)(a) ECT. The provision sets out that each contracting party gives its unrestricted consent to international arbitration. Based on Article 31 of the WCL as well as the CJEU's decisions in *Achmea*, *Komstroy* and statements of the EU member states on the consequences of Achmea, the arbitral tribunal concluded that Art 26(3)(a) ECT could not be interpreted without reference to EU law and that due to the primacy of EU law the the Spanish offer of arbitration is invalid. The existing conflict of norms was therefore not to be resolved

by means of lex posterior or lex specialis, but by means of lex superior.

Enforcement and Domestic Courts in the EU follow *Achmea*

The CJEU affirmed recently in *European Food* that the European Commission has the competence to examine damages awarded in intra-EU arbitrations according to state aid law, even if the actions concerned were decided before the accession of the state concerned to the EU. It was also stated that in these cases (i.e. also in ISCID proceedings) the *Achmea* case law has to be taken into account.

In addition, domestic courts in the EU (namely in Sweden and Luxembourg) have refused enforcement of an ICSID award on the basis of the CJEU case law, arguing that enforcement would violate the duty of loyal cooperation under EU law. In contrast, the UK Supreme Court and a US appeals court ruled otherwise. Within the ICSID system itself, however, the objection of questionable enforceability within the EU was rejected in the context of an annulment procedure.

Conclusion

In a first reaction to *Green Power*, ICSID tribunals have so far rejected the arguments raised. It will remain to be seen how tribunals will deal with the enforcement issues within EU states, and likewise how domestic courts in non-EU states will react. Considering the primacy and autonomy of the EU legal order in the eyes of the CJEU, it is only understandable for practical reasons that tribunals will have to find a pragmatic solution to this conflict between international law obligations and EU law.

Other Developments
European Union

DAC 7 - The Exchange of Tax Information for Businesses with Digital Platforms in the European Union

By Amedeo Rizzo and Martina Acciaro

The role of the digitalization of the economy has become prominent over the years and has been recently accelerated by the COVID-19 pandemic. According to the most recent European Investment Bank (EIB) Investment Survey, in the EU, 46% of firms have increased their level of digitalization after the pandemic[33]. This phenomenon originates critical issues for tax authorities, as digital activities are often outside the boundaries of the tax regulations, which are mainly suited for traditional business models.

Digital platforms are characterized by a cross-border dimension that allows them to trade globally without a physical presence. Therefore, identifying where the income is earned by those kinds of businesses becomes difficult, and tax administrations end up having insufficient information. As a response, some states have introduced unilateral reporting obligations. However, this creates unequal conditions among operators within the EU internal market. Aiming at regulating and harmonizing those situations, on March 22, 2021, the EU Council approved the Directive 2021/514/EU[34] on the exchange of tax information, also known as DAC 7.

How does the DAC 7 work?

Aspiring at protecting the competitiveness of EU operators, the scope of DAC 7 is extended to all countries, and not only to Member States. Therefore, the Directive will impact, in different ways, both EU digital platforms and non-EU digital platforms. All the following provisions shall be applied from January 1, 2023.

EU operators

According to the Directive, EU platform operators will have to cooperate with tax authorities, collecting information about each

[33] European Investment Bank (2022), "Digitalisation in Europe 2021-2022: Evidence from the EIB Investment Survey". https://www.eib.org/attachments/publications/digitalisation_in_europe_2021_2022_en.pdf

[34] https://eur-lex.europa.eu/eli/dir/2021/514/oj

platform's sellers. In essence, DAC 7 requires the communication of

- Personal data of the platform operator;
- Personal data of the sellers.

After the collection, platform operators shall furnish information to the competent tax authority, which will *automatically* exchange it with other EU tax authorities.

In order for the Directive to be functional, penalties have to be provided by Member States to non-complying subjects. Despite the arbitrariness of these sanctions, the criteria adopted by the EU require them to be effective and proportionate.

Non-EU operators

The treatment of non-EU platform operators depends on the State where the platform operator is a tax resident. If a non-EU jurisdiction has an information exchange agreement with the EU, equivalent to DAC 7, the non-EU platform operators are not required to comply with the Directive. In all the other cases, the non-EU tax administration shall provide the information requested by the Directive on their platform operators. Where the non-EU tax administration is not willing to cooperate, foreign platform operators shall register in the EU and furnish their own data.

If a registered foreign platform does not provide information, the platform operator's registration will be revoked between 30 and 90 days after the second reminder made by the Member State. The types of sanctions applied in such cases are discretionary to the Member States, despite the difficulty of applying effective harmonized countervailing measures towards non-EU platforms.

Digital platforms and in-scope businesses

What is really new in the EU Directive is the huge range of businesses that will be hit by the legislation. *Prima facie*, this is immediately noticeable comparing the DAC 7 with the Model Rules developed by the OECD. While the OECD Model Rules identify the relevant activities only as the rental of immovable property and personal services, the EU opts for the inclusion of any sale of goods and the rental of any means of transport. Second, the broad scope of the legislation can be appreciated in the definition of "platform", provided by the DAC 7 as: "*any software, including a website [...], accessible by users and allowing Sellers to be connected to other users to carry out a Relevant Activity, directly or indirectly, to such users*". This definition includes digital industries (such as live streaming apps, tech companies providing food delivery platforms, virtual marketplaces, and online travel agents), but also many other industries that make use of e-commerce. According to the *European E-Commerce Report 2022*, EU citizens purchase online various product categories. For example, 68% of clothes, shoes or accessories, 38% of physical multimedia, and 27% of cosmetics, beauty or wellness products are bought online.

Automatic exchange of information in the US and the OECD

Automatic exchange of information was already introduced by the US in 2010 through the "Foreign Account Tax Compliance Act" (FATCA). The US managed to enforce the collaboration of foreign tax administrations and foreign financial institutions to collect information about US citizens' offshore investments (i.e., personal data and foreign financial accounts).

At the OECD level, the Common Reporting Standard (CRS), which requires financial institutions to exchange financial accounts information, was approved by the OECD Council in 2014 and is going through an implementation stage.

However, those measures are both very different from the DAC 7 as they do not aim specifically at receiving information from digital activities. Even when this information accidentally falls into the scope of the exchange of tax information, it does not bear the same level of specificity concerning platforms' operators and sellers.

Conclusion

The reporting obligation should facilitate the multilateral automatic exchange of information and should help the EU fight tax evasion in businesses with a strong digital presence. Nevertheless, the DAC 7 does not provide a quantitative limit, under which the obligation would be waived. This implies high, and often pointless, compliance costs for small businesses which is an unintended consequence of the Directive.

All in all, despite some issues, the DAC 7 constitutes a step forward to regulate digital businesses' taxation, which increases tax transparency and administrative cooperation among EU Member States. Additionally, including also non-EU operators, the DAC 7 could embody an encouragement for non-EU countries to prioritize their rules on digital businesses' taxation and implement, overall, more effective systems.