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. 1/2020 (March 19, 2020)

Contributors:

Elif Kiesow Cortez, Jonathan Cardenas,
Mauritz Kop, Odysseas G. Repousis,
Pratyush Nath Upreti

Editor-in-chief: Juha Vesala

Contents

About the contributors

Elif Kiesow Cortez is a senior lecturer and researcher in data protection and privacy regulation in the International and European Law Program at The Hague University of Applied Sciences (THUAS), Netherlands. Elif is the coordinator of the Legal Technology Minor and the Cybersecurity Minor at THUAS. Before joining THUAS, Elif was a John M. Olin Fellow in Law and Economics at Harvard Law School. Elif's doctoral research at the Institute of Law and Economics, University of Hamburg, Germany, was funded by the German Research Association (DFG). During her doctoral studies, Elif was a visiting fellow at Harvard Business School and a visiting scholar at Berkeley School of Law. Elif holds undergraduate degrees in law and in economics and her research is focused on utilizing economic analysis of law to provide recommendations for solving cooperation problems between public and private actors in the domains of data protection and privacy. Since 2018, Elif is an advisory board member for the CIPP/E Exam Development Board of the IAPP. Elif has been a TTLF Fellow since 2020.

Jonathan Cardenas is a corporate associate in Crowell & Moring's Washington, D.C. office, and is also a TTLF Fellow. Prior to joining Crowell & Moring, Jonathan served as a postdoctoral fellow with the Information Society Project at Yale Law School. Jonathan received a J.D. from New York University School of Law, where he was a Jacobson Leadership Program in Law & Business Scholar, and where he served as managing editor of the NYU Journal of Law & Business. He received an M.Phil. in international relations from the University of Cambridge and a B.A. in political science, summa cum laude, from the University of Pennsylvania.

Mauritz Kop is Founder of MusicaJuridica and strategic intellectual property lawyer at AIRecht in Amsterdam, The Netherlands. He delivered copyright expertise to the European Parliament during the EU Copyright Directive legislative process, focusing on online content platforms, human rights, multi-territorial licensing and market entry of tech start-ups. Mauritz is a member of the European AI Alliance (European Commission), the Dutch Copyright Society (VvA), CLAIRE (Confederation of Laboratories for Artificial Intelligence Research in Europe), the Dutch AI Coalition (NL AIC) and the ECP|Platform for the Information Society. His expert commentary has appeared in numerous outlets, including NRC Handelsblad, RTL Nieuws, NPO2 NTR, BNR Nieuwsradio, Radio Veronica and Leiden Centre of Data Science (LCDS). Mauritz is columnist Legal Dimension of Transformative Tech at Platform VerderDenken.nl and guest lecturer Post Academic Intellectual Property Law at the Centre for Professional Legal Education (CPO), Radboud University Nijmegen. Here he provides legal training to judges, lawyers and legal professionals. Mauritz held a number of IP, music and technology law guest teaching positions at various Law Schools, such as Leiden University, Maastricht University and Utrecht University. He is author of numerous articles and blogs about legal and ethical aspects of exponential innovation in industrial sectors such as Healthcare, AgriFood and Entertainment & Art, and is a frequently asked international conference speaker on topics in the nexus of AI and Law. As a student, Mauritz was a Member of the Faculty of Law Curriculum Council at Maastricht University, where he redesigned the curriculum and helped to implement the Bachelor-Master system into the program. He studied intellectual property law, labor law and contract law at Stanford Law School, Maastricht University and VU University Amsterdam. His present interdisciplinary, comparative research focuses on Human Centered AI & IP and sustainable disruptive innovation policy pluralism. In his free time Mauritz enjoys playing tennis, yachting, composing, producing and performing music. He has been a TTLF Fellow since 2019.

Odysseas Repousis is an associate in Quinn Emanuel's London office and a member of the litigation and international arbitration practice groups. Prior to joining Quinn Emanuel, Odysseas taught and conducted research at Harvard Law School and the University of Hong Kong, worked at the International Chamber of Commerce and the European Commission (at the Directorate General for Trade) and held research positions with the British Institute of International and Comparative Law, the Hong Kong International Arbitration Centre and the United Nations International Law Commission. Odysseas has a Master of Laws Degree from Harvard Law School and a Ph.D. from the University of Hong Kong. He has received several prizes and awards for his professional and academic work, including the Harvard University Scholarship and the Li Ka Shing Prize (also known as the Best Ph.D. Thesis Award) and he is recognized as a Future Leader in Litigation by Who's Who Legal 2019. Odysseas has spoken and written extensively on international arbitration and litigation topics, and has delivered lectures at universities in the United States, Europe and Hong Kong. Odysseas has been a TTLF Fellow since 2019.

Pratyush Nath Upreti is a lawyer admitted to the Nepal Bar Council. He is a Doctoral Researcher at Sciences Po Law School, Paris and currently a visiting research fellow at the Max Planck Institute for Innovation and Competition in Munich, Germany. Previously, he was a visiting researcher at the Centre for Intellectual Property Policy & Management (CIPPM) of Bournemouth University in the UK. He has taught Intellectual Property and International Trade Law at the Europe-North America and the Europe-Asia Programs of Sciences Po. Pratyush also serves as a member on the editorial board for the Global Trade and Customs Journal published by Kluwer Law International. He holds a BSc. LL.B.(Hons) degree from KIIT University, India, and an LL.M. degree from Maastricht University, Netherlands as a UM High Potential Scholar. His interests include intellectual property law, international investment law, and WTO related issues. He has been a TTLF Fellow since June 2018.

Intellectual property

United States

IP Chapter in the First Phase of US-China Trade Deal

By Pratyush Nath Upreti

On 15th January 2020, the first phase of the ‘Economic and Trade Agreement’ [here after trade deal] between the United States (US) and China was released.[1] The draft came in light of recent proxy trade wars between two countries where both the countries imposed tariffs and retaliatory tariffs among each other’s. The general outline of phase one of the trade deal was conceptualized in an 86 page long ‘Fact Sheet’ released in December 2019. This note provides a succinct overview of some key provisions of the IP Chapter.

Some observation

IP Chapter is the first chapter in the trade deal. In general, the Chapter is divided into eleven sections that cover areas related to trade secrets, patents, IP enforcement, e-commerce, geographical indications, trademarks, copyright, and related rights among others.

The section on ‘Trade Secrets and Confidential Business Information’ incorporates a broad definition of trade secrets. It covers ‘concerns or relates’ to trade secrets and almost any other information of commercial value, which disclosure can have the effect to cause ‘substantial harm’ to the ‘competitive position’ of the complainant. In addition, there is a key provision on the burden of proof. The relevant provision emphasizes that if trade secrets holder provides *prima facie* evidence, including circumstantial evidence of a reasonable indication of trade secret misappropriation, the burden of proof will shift to the accused party in civil proceeding (Article 1.5). Additionally, there should be no requirement to establish actual losses as a prerequisite to initiating a criminal investigation (Article 1.6). Another noteworthy section is on ‘Pharmaceutical-Related Intellectual Property’, that obliges China to create a system of ‘pre-market notification’ where it requires to provide notice to the patent holder, licensee or holder of marketing approval about people seeking to market generic version during the term of applicable patent, approved product or method of use for seeking approval (Article 1.11).

[1] See Pratyush Nath Upreti and María Vásquez Callo-Müller, ‘Phase One US-China Trade Deal: What Does It Mean for Intellectual Property?’ (2020) 4 GRUR International: Journal of European and International IP Law (forthcoming).

Besides, the IP Chapter commits China to allow disagreement to the US or other trading partners on China's list of geographical indications agreed in the agreement with another trading partner (Article 1.15). The relevant section obliges China to take measures to reduce online infringement including 'notice and takedown'. China commits to requiring 'expeditious takedowns', 'eliminate liability for takedown notices submitted in good faith', among others (Article 1.13).

To conclude, IP chapter departs from the recent US-led trade negotiations in Mexico and Canada (USMCA) and the earlier version of the Trans-Pacific Partnership Agreement. The general reading of the IP chapter gives the impression that the ultimate aim of the US was to bring structural reforms in China's IP regime through transplanting the US IP norms.

Intellectual Property

European Union

Machine Learning & EU Data Sharing Practices

By Mauritz Kop[2]

Introduction

Data sharing or rather the ability to analyse and process high quality training datasets (*corpora*) to teach an Artificial Intelligence (AI) model to learn, is a prerequisite for a successful Transatlantic AI ecosystem. But what about intellectual property (IP) and data protection?

In our turbulent technological era, tangible information carriers such as paper and storage media are declining in importance. Information is no longer tied to a continent, state or place. Information technology such as AI is developing at such a rapid, exponential pace that the legal problems that arise from it are to a large extent unpredictable.

1. Legal dimensions of data

Data, or information, has a large number of legal dimensions.[3] Data sharing is associated with IP law (right to prohibit and reimburse), fundamental rights (privacy, data protection, freedom of expression and other constitutional rights)[4], fiscal law (taxation), contract law and international commercial law (e-commerce, trade treaties, anti-trust law, consumer protection).[5] In addition, the handling of

[2] Mauritz Kop, Stanford Law School TTLF Fellow, Stanford University; Managing Partner at AIRecht, Amsterdam, The Netherlands. Correspondence: advies@airecht.nl. The author would like to thank Mark Lemley, Begoña Gonzalez Otero, Teresa Quintel, Suzan Slijpen and Nathalie Smuha for valuable remarks on an earlier draft of this article, and Christophe Geiger for his lecture on *Big Data, Artificial Intelligence, Freedom of Information and* the TDM exception, organized by IViR, 10 March 2020.

[3] Data and information are not always interchangeable terms. From a European trade secrets perspective, it is not clear whether data or datasets fulfill the requirements of Article 2(1) of the EU Trade Secrets Directive (TSD). When data is mentioned in the TSD, the terms seems to be not understood as “datasets” but rather in the context of customer/supplier lists – “commercial data” in recital 2 or “personal data” in Article 9(4). The TSD was not developed with the data-driven economy in mind, but rather on the information society (recitals 1 and 4).

[4] Privacy and data protection are not always interchangeable terms. Privacy is a human right as enshrined in Article 12 of the Universal Declaration of Human Rights.

[5] See for international commercial law aspects: Kristina Irion & Josephine Williams (2019). ‘Prospective Policy Study on Artificial Intelligence and EU Trade Policy’. Amsterdam: The Institute for information Law (IViR) 2019. See for consumer protection: Gabriele Accardo and Maria Rosaria Miserendino, ‘Big Data: Italian Authorities Published Guidelines and Policy Recommendation on Competition, Consumer Protection, and Data Privacy Issues’, TTLF Newsletter on Transatlantic Antitrust and IPR Developments Stanford-Vienna Transatlantic Technology Law Forum, Stanford University, 2019 Volume 3-4. https://ttlfnews.wordpress.com/2019/11/29/big-data-italian-authorities-published-guidelines-and-policy-recommendation-on-competition-consumer-protection-and-data-privacy-issues/. See for unfair competition law, data sharing and social media platforms: Catalina Goanta, ‘Facebook’s Data Sharing Practices under Unfair Competition Law’, TTLF Newsletter on

personal data has ethical, social and techno-philosophical facets.

Legal ownership of data does not exist

In most European countries, the law of property is a closed system.[6] This means that the number of proprietary rights *in rem*, which are rights enforceable against everyone, are limited by law. Legal ownership of data therefore does not yet exist. From a property law point of view, data cannot be classified as ''*res*'', as an intangible good or as a thing in which property rights can be vested. Data does have proprietary rights aspects and represents value.

Data that represent IP subject matter

Data that represent IP subject matter are protected by IP rights.[7] Data that embody original literary or artistic works are protected by copyright. New, non-obvious and useful inventions represented by data are protected by patents. Data that epitomize independently created new and original industrial designs are safeguarded by design rights.[8] Confidential data that have business or technological value are protected by trade secret rights.[9]

Sui generis database rights

Hand-labelled, annotated machine learning training datasets are awarded with either a database right or a *sui generis* database right in Europe.[10] Although the 1996 Database Directive was not developed with the data-driven economy in mind, there has been a general tendency of extensive interpretation in favor of database

Transatlantic Antitrust and IPR Developments Stanford-Vienna Transatlantic Technology Law Forum, Stanford University, 2018 Volume 2. https://ttlfnews.wordpress.com/2018/06/08/facebooks-data-sharing-practices-under-unfair-competition-law/ See for competition law as a driver for digital innovation and its relationship with IP law: Josef Drexl, 'Politics, digital innovation, intellectual property and the future of competition law', Concurrences Review 4 (2019), 2-5. https://www.concurrences.com/en/review/issues/no-4-2019/foreword/politics-digital-innovation-intellectual-property-and-the-future-of-competition

[6] All European Member States have civil law systems. Great Britain, as the USA, has a common law system.

[7] WIPO Conversation on Intellectual Property (IP) and Artificial Intelligence (AI), Second Session,
Draft Issues Paper on Intellectual Property Policy and Artificial Intelligence, prepared by the WIPO Secretariat, December 13, 2019 https://www.wipo.int/about-ip/en/artificial_intelligence/policy.html

[8] *Ibid*. See also: https://www.wipo.int/meetings/en/doc_details.jsp?doc_id=470053

[9] WIPO is planning to launch a digital time stamping service that will help innovators and creators prove that a certain digital file was in their possession or under their control at a specific date and time. See: 'Intellectual property in a data-driven world', WIPO Magazine October 2019 https://www.wipo.int/wipo_magazine/en/2019/05/article_0001.html The time stamping initiative is a digital notary service that resembles the BOIP i-Depot, see https://www.boip.int/en/entrepreneurs/ideas

[10] Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases (Database Directive): https://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31996L0009:EN:HTML For an analysis of the rules on authorship and joint authorship of both databases and database makers' sui generis rights, and how to overcome potential problems contractually see: Michal Koščík & Matěj Myška (2017), 'Database authorship and ownership of sui generis database rights in data-driven research', International Review of Law, Computers & Technology, 31:1, 43-67, DOI: 10.1080/13600869.2017.1275119

protection.[11] A database right can be qualified as either a neighboring (ancillary or related) right (however shorter in duration i.e. 15 years), or a true *sui generis* IP right, but not as a full copyright. A *sui generis* database right is an IP right with characteristics of a property right, and is awarded after a substantial investment in creating and structuring the database, be it money or time, has been made. Businesses usually consider hand-labelled, tagged training *corpora* to be an asset that they can license or sell to another company. This applies to the AI system's output data as well. As all IP rights, (*sui generis)* database rights are subject to exhaustion.[12] In the USA, no *sui generis* database right exists on augmented input or output data.[13] What Europe and the USA do have in common, is that any existing IP rights on input data need to be cleared before processing.

Feeding training data to the machine qualifies as a reproduction of works, and requires a license.[14] The training *corpus* usually consists of copyrighted images, videos, audio, or text. If the training *corpus* contains non-public domain (copyrighted) works or information protected by database rights -and no text and datamining (TDM)[15] exception applies- *ex ante* permission to use and process must be obtained from the rightsholders (for both scientific, commercial and non-commercial training purposes).

Clearance of machine learning training datasets

Unlicensed (or uncleared) use of machine learning input data potentially results in an avalanche of copyright (reproduction right) and database right (extraction right) infringements.[16] Some content owners will have an incentive to prohibit or monetize

[11] See also CJEU, Case C-490/14 Verlag Esterbauer, The CJEU notes that the term "database" is to be given a wide interpretation. In the case of hand-labelled data for supervised machine learning, application of the Database Directive is not really straight forward. The Database Directive does not distinguish between hand and machine coding in what it protects, only between digital and analogue databases. It has been evaluated for the second time in 2018, see https://ec.europa.eu/digital-single-market/en/protection-databases

[12] Mezei, Péter, Digital First Sale Doctrine Ante Portas -- Exhaustion in the Online Environment (June 7, 2015). JIPITEC – Journal of Intellectual Property, Information Technology and E-Commerce Law, Vol. 6., Issue 1., p. 23-71, 2015. Available at SSRN: https://ssrn.com/abstract=2615552. This rule has two exceptions: online transmission of the database and lending or rental of databases do not result in exhaustion.

[13] Bernt Hugenholtz, 'Something Completely Different: Europe's Sui Generis Database Right', in: Susy Frankel & Daniel Gervais (eds.), The Internet and the Emerging Importance of New Forms of Intellectual Property (2016), 205-222. See also SCOTUS landmark decision Feist: *Feist Publications, Inc., v. Rural Telephone Service Company, Inc.*, 499 U.S. 340 (111 S.Ct. 1282, 113 L.Ed.2d 358), No. 89-1909. https://www.law.cornell.edu/supremecourt/text/499/340

[14] See also James Grimmelmann, 'Copyright for Literate Robots' (101 Iowa Law Review 657 (2016), U of Maryland Legal Studies Research Paper No. 2015-16) 678, https://scholarship.law.cornell.edu/facpub/1481/. Access to out-of-commerce works held by cultural heritage institutions also requires clearance. In Europe, this license can be obtained from collective rights organisations (Article 8 CDSM Directive).

[15] The non-technologically neutral definition of 'text and data mining' in the CDSM Directive is '*any automated analytical technique aimed at analysing text and data in digital form in order to generate information which includes but is not limited to patterns, trends and correlations*'.

[16] Whether for research purposes or for commercial product development purposes.

data mining.[17] Three solutions that address the input (training) data copyright clearance problem and create breathing room for AI developers, are the implementation of a broadly scoped, mandatory TDM exception (or even a right to machine legibility)[18] covering all types of data (including news media) in Europe,[19] the Fair Learning principle in the USA[20] and the establishment of an online clearinghouse for machine learning training datasets. Each solution promotes the urgently needed freedom to operate and removes roadblocks for accelerated AI-infused innovation.

Three solutions

The TDM exceptions where originally not created with machine learning training datasets in mind. Prominent scholars advocating the introduction of robust TDM provisions to make Europe fit for the digital age and more competitive vis-a-vis the United States and China are Bernt Hugenholtz and Christophe Geiger. The '[Joint Comment to WIPO on Copyright and Artificial Intelligence]' addresses *-inter alia-* challenges related to machine learning and the much needed freedom to use training *corpora*. This 'amicus brief' discusses solutions such as individual and collective TDM licenses/exceptions, whether for commercial or scientific objectives.

On the other side of the Ocean, Mark Lemley and Bryan Casey introduced the concept of Fair Learning.[21] The authors contend that AI systems should generally be able to use databases for training whether or not the contents of that database are copyrighted. Permitting copying of works for non-expressive purposes will be -in most cases- a properly balanced, elegant policy-option to remove IP obstacles for training machine learning models and is in line with the idea/expression dichotomy.

A third solution could be the establishment of an online clearinghouse for machine learning training datasets. An ex ante or ex post one-stop-shop resembling a collective rights society, however on the basis of a sui generis compulsory licensing system. A framework that would include a right of remuneration for rights holders, but without the right to prohibit data usage for commercial and scientific machine learning purposes.[22] With a focus on permitted, free flow of interoperable data.

Public versus private data

Another legal dimension that we can distinguish is on the one hand public (in the hands of the government) machine

[17] Bernt Hugenholtz, The New Copyright Directive: Text and Data Mining (Articles 3 and 4), Kluwer Copyright Blog (July 24, 2019), http://copyrightblog.kluweriplaw.com/2019/07/24/the-newcopyright-directive-textand-data-mining-articles-3-and-4/?print=print Article 4 CDSM allows right holders to opt out of the TDM exception.

[18] Ducato, Rossana and Strowel, Alain M., 'Limitations to Text and Data Mining and Consumer Empowerment: Making the Case for a Right to Machine Legibility' (October 31, 2018). CRIDES Working Paper Series, 2018. Available at SSRN: https://ssrn.com/abstract=3278901

[19] Geiger, Christophe and Frosio, Giancarlo and Bulayenko, Oleksandr, 'The Exception for Text and Data Mining (TDM) in the Proposed Directive on Copyright in the Digital Single Market - Legal Aspects' (March 2, 2018). Centre for International Intellectual Property Studies (CEIPI) Research Paper No. 2018-02.

[20] Lemley, Mark A. and Casey, Bryan, Fair Learning (January 30, 2020). Available at SSRN: https://ssrn.com/abstract=3528447

[21] *Ibid.* (*supra* note 19)

[22] See also WIPO (*supra* note 6)

generated (non) personal data, and private (in the hands of the business community) machine generated (non) personal data. By machine generated data, we mean in particular information and data that are continuously generated by edge devices in the Internet of Things (IoT).[23] These edge devices are connected via edge (or fod) nodes (transmitters) to data centers that together with edge servers form the cloud. This architecture is known as edge computing.

Legal reform

Mandatory TDM exceptions are a sine qua non for machine learning in Europe.[24] A right of fair, remunerated text and data use to train an AI system needs to be mandatory and without opt outs. Would a broadly scoped TDM exception be an optional limitation, with room for Member States to implement their own rules, the Digital Single Market will become fragmented instead of harmonized. A right to machine legibility that drastically improves access to data, will greatly benefit the growth of the European AI-ecosystem.[25]

Besides implementing broader scoped TDM exceptions, it is opportune that the EU Database Directive 96/9/EC shall be reformed by the EU Commission to prevent that data generated by connected edge devices qualifies for *sui generis* database right protection. Edge computing data must not be monopolized.[26]

2. Technical dimensions of data in machine learning

Most AI models need centralized data. In the current, dynamic field of machine learning[27], hand-labelled training datasets are a sine qua non for supervised machine learning, which uses regression and classification techniques to solve its prediction and optimization problems. This process mimics biological cognition. In contrast, unsupervised machine learning, which utilizes association and clustering (pattern recognition) techniques, uses unlabelled (unstructured) datasets as an input to train its algorithms to discover valuable regularities in digital information. Semi-supervised learning employs a combination of structured and unstructured training datasets to feed our thinking machines.

Data in machine learning can be discrete or continuous, numerical and categorical. AI systems that utilize deep learning techniques for predictive analysis and optimization, contain deep layers of

[23] Such as in smart cities, smart energy meters, Wi-Fi lamps and user gadgets including smart wearables, televisions, smart cameras, smartphones, game controllers and music players.

[24] Countries with more room in their legal frameworks i.e. less legal barriers to train machine learning models are Switzerland, Canada, Israel, Japan and China.

[25] Ducato and Strowel (*supra* note 17)

[26] Such an innovation friendly reform directly impacts the Digital Single Market. It is to be hoped that the necessary policy space to realize these much needed revisions exists in Brussels.

[27] For the latest scientific breakthrough in machine learning methods see: Matthew Vollrath, 'New machine learning method from Stanford, with Toyota researchers, could supercharge battery development for electric vehicles', February 19, 2020 https://news.stanford.edu/2020/02/19/machine-learning-speed-arrival-ultra-fast-charging-electric-car/ According to Stanford professors Stefano Ermon and William Chueh the machine isn't biased by human intuition. The researcher's ultimate goal is to optimize the process of scientific discovery itself.

artificial neural networks, with representation learning.[28] Artificial deep neural networks (ANN's and DNN's) rudimentarily mimic the architecture of human biological brains and are comprised of simplified, artificial neuron layers. Anno 2020 DNN's do not yet have axon's, soma, dendrites, neurotransmitters, plasticity, cerebral cortices and synaptic cores. In the field of AI, data mining, statistics, engineering and neuroscience converge.

Deep reinforcement learning

Reinforcement learning does not require existing input datasets. Instead, the model learns from data from simulations and games using a reward system based on continuous feedback. Deep reinforcement learning systems, such as AlphaGo, are not easy to train. Too many correlations in the data interfere with its goal-oriented algorithms' stable learning process. Inference applies the capabilities of a pre-trained deep learning system to new datasets, to predict its output in the form of new, useful real-world values and information.

Transfer learning is a machine learning method that seeks to apply a certain solution model for a particular problem to another, different problem. Applying a pre-trained model to new (and smaller) datasets can turn a one trick pony into the ultimate synthetic multitasker.

Evolutionary computing uses genetic optimization algorithms inspired by neo-Darwinian evolution theory.[29] Genetic algorithms can be used standalone[30], or to train ANN's and DNN's and to identify suitable training *corpora*.

The approaches described above are all centralized machine learning techniques. Federated learning, in contrast, trains algorithms that are distributed over multiple decentralized edge devices in the Internet of Things. These mobile devices -such as your smartphone- contain local data samples, without exchanging their data samples. The interconnected IoT devices collaboratively train a model under a central server.[31] Federated Learning is a scalable, distributed machine learning approach which enables model training on

[28] An example of such an AI system is a generative adversarial network, which consists of two different neural networks competing in a game.

[29] Drexl, Josef and Hilty, Reto and Beneke, Francisco and Desaunettes, Luc and Finck, Michèle and Globocnik, Jure and Gonzalez Otero, Begoña and Hoffmann, Jörg and Hollander, Leonard and Kim, Daria and Richter, Heiko and Scheuerer, Stefan and Slowinski, Peter R. and Thonemann, Jannick, Technical Aspects of Artificial Intelligence: An Understanding from an Intellectual Property Law Perspective (October 8, 2019). Max Planck Institute for Innovation & Competition Research Paper No. 19-13. Available at SSRN: https://ssrn.com/abstract=3465577

[30] For example in NASA Antenna. See: Hornby, Greg & Globus, Al & Linden, Derek & Lohn, Jason. (2006), 'Automated Antenna Design with Evolutionary Algorithms', Collection of Technical Papers - Space 2006 Conference. 1. 10.2514/6.2006-7242. https://ti.arc.nasa.gov/m/pub-archive/1244h/1244%20(Hornby).pdf

[31] Kairouz, Peter & McMahan, H. & Avent, Brendan & Bellet, Aurélien & Bennis, Mehdi & Bhagoji, Arjun & Bonawitz, Keith & Charles, Zachary & Cormode, Graham & Cummings, Rachel & D'Oliveira, Rafael & El Rouayheb, Salim & Evans, David & Gardner, Josh & Garrett, Zachary & Gascón, Adrià & Ghazi, Badih & Gibbons, Phillip & Gruteser, Marco & Zhao, Sen. (2019). 'Advances and Open Problems in Federated Learning', https://arxiv.org/pdf/1912.04977.pdf

a large *corpus* of decentralized data.[32] ‘'*Federated learning embodies the principles of focused data collection and minimization, and can mitigate many of the systemic privacy risks and costs resulting from traditional, centralized machine learning and data science approaches.*'’[33] It brings the code to the data, instead of bringing the data to the code.[34] In other words, there is no need for sharing data.

3. Data: contracts, property law and trade secrets

IP on training data and data management systems is subject to both property law aspects and proprietary rights *in rem* that are enforceable against everyone. Data is not a purely immaterial, non-physical object in the legal (not the natural-scientific) meaning of the word. However, if a party to a dataset transaction has acquired a contractual claim right in exchange for material benefits provided by him, there is a proprietary right. This proprietary right *in rem* is subject to transfer, license and delivery.

The attitude of the parties, and their legal consequence-oriented behaviour when concluding contracts about datasets and their proprietary aspects may perhaps prevail over the absence of a clear legal qualification of data[35] (or information) in the law. In this case, party intentions go beyond the legal void.[36] In other words, legislative gaps can be remedied by contracts.[37]

Legal ownership, or property, is different from an IP right. IP is a proprietary right *in rem*. An IP right can entail a right to use data, in the form of a license.

Extra layers of rights will not bring more innovation

Raw non personal machine generated data are not protected by IP rights.[38] Introducing an absolute data property right or a (neighboring) data producer right for augmented machine learning training datasets, or other classes of data, is not opportune. Economic literature has made

[32] Bonawitz, Keith & Eichner, Hubert & Grieskamp, Wolfgang & Huba, Dzmitry & Ingerman, Alex & Ivanov, Vladimir & Kiddon, Chloe & Konečný, Jakub & Mazzocchi, Stefano & McMahan, H. & Overveldt, Timon & Petrou, David & Ramage, Daniel & Roselander, Jason. (2019), ‘Towards Federated Learning at Scale: System Design’, https://arxiv.org/pdf/1902.01046.pdf

[33] *Ibid*. (*supra* note 30)

[34] *Ibid*. (*supra* note 31)

[35] Tjong Tjin Tai, Eric, ‘Een goederenrechtelijke benadering van databestanden’, Nederlands Juristenblad, 93(25), 1799 - 1804. Wolters Kluwer, ISSN 0165-0483. The author contends that data files should be treated analogous to property of tangible objects within the meaning of Book 3 and 5 of the Dutch Civil Code, as this solves several issues regarding data files.

[36] Until new European legislation creates clarity, gaps and uncertainties will have to be filled by the courts.

[37] Unfortunately, licensing large datasets commercially almost never works out in practice.

[38] For further reading about IP and property rights vested in private data see Begonia Otero, ‘Evaluating the EC Private Data Sharing Principles: Setting a Mantra for Artificial Intelligence Nirvana?’, 10 (2019) JIPITEC 87 para 1. https://www.jipitec.eu/issues/jipitec-10-1-2019/4878. For non-personal machine generated data see P. Bernd Hugenholtz, ‘Data Property: Unwelcome Guest in the House of IP (25 August 2017), http://copyrightblog.kluweriplaw.com/2017/08/25/data-producers-right-unwelcome-guest-house-ip/ and Ana Ramalho, ‘Data Producer's Right: Power, Perils & Pitfalls’ (Paper presented at Better Regulation for Copyright, Brussels, Belgium 2017)

clear that there are no convincing economic, or innovation policy arguments for the introduction of a new layer of rights, especially due to the absence of an incentive and reward problem for the production and analysis of datasets.[39]

Moreover, additional exclusive rights will not automatically bring more innovation. Instead, it will result in overlapping IP rights and database right thickets. [40] The introduction of a sui generis system of protection for AI-generated Creations & Inventions is -in most industrial sectors- not necessary since machines do not need incentives to create or invent. [41] Where incentives are needed, IP alternatives exist. Finally, there are sufficient IP instruments to protect the various components of the AI systems that process data, create and invent. [42] Because of theoretical cumulation of copyrights, patents, trade secrets and database rights, protection overlaps may even exist.[43]

Public Property from the Machine

Non-personal data that is autonomously generated by an AI system and where upstream and downstream no significant human contribution is made to its creation, should fall into the public domain. [44] It should be open data, excluded from protection by the Database Directive, the Copyright Directive [45] and the Trade Secrets Directive.

These open, public domain datasets can then be shared freely without having to pay compensation and without the need for a license. No monopoly can be established on this specific type of database. I would like to call these AI Creations "*Res Publicae ex Machina*" [46] (Public Property from the Machine). Their classification can be clarified by means of an official public domain status stamp or marking (PD Mark

[39] Kerber, Wolfgang, 'A New (Intellectual) Property Right for Non-Personal Data? An Economic Analysis' (October 24, 2016). Gewerblicher Rechtsschutz und Urheberrecht, Internationaler Teil (GRUR Int), 11/2016, 989-999. See also Landes, William M., and Richard A. Posner. "An Economic Analysis of Copyright Law." The Journal of Legal Studies, vol. 18, no. 2, 1989, pp. 325–363. JSTOR, www.jstor.org/stable/3085624

[40] James Boyle, The Public Domain: Enclosing the Commons of the Mind, (Orange Grove Books 2008) 236

[41] Kop, Mauritz, AI & Intellectual Property: Towards an Articulated Public Domain (June 12, 2019). Forthcoming Texas Intellectual Property Law Journal 2020, Vol. 28. Available at SSRN: https://ssrn.com/abstract=3409715 The legal concept of *Res Publicae ex Machina* is a catch-all solution.

[42] Exhaustion of certain IP rights may apply, see note 11. See also Shubha Ghosh and Irene Calbol, '*Exhausting Intellectual Property Rights: A Comparative Law and Policy Analysis',* (CUP 2018), 101

[43] *Ibid*. Kop (*supra* note 40). See also Deltorn, Jean-Marc and Macrez, Franck, Authorship in the Age of Machine learning and Artificial Intelligence (August 1, 2018). In: Sean M. O'Connor (ed.), The Oxford Handbook of Music Law and Policy, Oxford University Press, 2019 (Forthcoming) ; Centre for International Intellectual Property Studies (CEIPI) Research Paper No. 2018-10. Available at SSRN: https://ssrn.com/abstract=3261329

[44] This means that there should be no sui generis database right vested in such datasets in Europe. No contract or license will be required for the consent of the right holders for analysis, use or processing of the data.

[45] Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC (CDSM Directive), https://eur-lex.europa.eu/eli/dir/2019/790/oj

[46] Kop (*supra* note 40). The legal concept of *Res Publicae ex Machina* is a catch-all solution.

status).[47] Freedom of expression and information are core democratic values that -together with proportionality- should be internalized in our IP framework. Reconceptualizing and strengthening the public domain paradigm within the context of AI, data and IP is an important area for future research.[48]

Data as trade secret

In practise however, to safeguard investments and monetize AI applications, companies will try hard either to keep the data a trade secret or to protect the overall database, whether it was hand-coded or machine generated. From an AI perspective, the various strategies to maximize the quality and value of a company's IP portfolio can differ for database rights, patents and trade secrets on the input and output of an AI system. Moreover, this strategy can differ per sector and industry (e.g. software, energy, art, finance, defence).

As legal uncertainty about the patentability of AI systems[49] is causing a shift towards trade secrets, legal uncertainty about the protection and exclusive use of machine generated databases is causing a similar shift towards trade secrets. Although it is not written with the data driven economy in mind, the large scope of the definition of a trade secret in the EU means that derived and inferred data can in theory be classified under the Trade Secrets Directive.[50] This general shift towards trade secrets to keep competitive advantages results in a disincentive to disclose information and impedes on data sharing.[51]

In an era of exponential innovation, it is urgent and opportune that both the Trade Secrets Directive, the Copyright Directive and the Database Directive shall be reformed by the EU legislature with the data-driven economy in mind.

4. EU open data sharing initiatives

Data can be shared between Government, Businesses, Institutions and Consumers. Within an industry sector or cross-sectoral.

Important European initiatives in the field of open data[52] and data sharing are: the Support Centre for Data Sharing (focused on data sharing practices), the European Data Portal (EDP, data pooling per industry

[47] Autonomously generated non personal datasets should be public domain.

[48] Hilty, Reto and Hoffmann, Jörg and Scheuerer, Stefan, Intellectual Property Justification for Artificial Intelligence (February 11, 2020). Draft chapter. Forthcoming in: J.-A. Lee, K.-C. Liu, R. M. Hilty (eds.), Artificial Intelligence & Intellectual Property, Oxford, Oxford University Press, 2020, Forthcoming; Max Planck Institute for Innovation & Competition Research Paper No. 20-02. Available at SSRN: https://ssrn.com/abstract=3539406 The article debates the question of justification of IP rights for both AI as a tool and AI-generated output in light of the theoretical foundations of IP protection, from both legal embedded deontological and utilitarian economic positions.

[49] Kop (*supra* note 40). Not opting for the patent route poses the risk of (bona fide) independent invention by someone else who does opt for the patent route instead of the trade secret strategy.

[50] Wachter, Sandra and Mittelstadt, Brent, 'A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI' (October 05, 2018). Columbia Business Law Review, 2019(1). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3248829

[51] Kop (*supra* note 40). Besides that, uncertainty about the scope of the TDM exceptions leads to litigation.

[52] For certain AI systems, open data should be required for safety reasons.

i.e. sharing open datasets from the public sector, the Open Data Europe Portal (ODP, sharing data from European institutions), the Free flow of non-personal data initiative (including the FFD-Regulation, cyber security and self-regulation) and the EU Blockchain Observatory and Forum.

A European initiative in the strongly related field of AI is the European AI Alliance, established by the EU Commission. An international project on AI and -inter alia- training data is the "AI and Data Commons" of the ITU (International Telecommunication Union).

EU Data Strategy

On February 19 2020 The EU Commission published its ‘EU Data Strategy’.[53] The EU aims to become a leading role model for a society empowered by data and will to that end create Common European Data Spaces in verticals such as Industrial Manufacturing, Health, Energy, Mobility, Finance, Agriculture and Science. An industrial package to further stimulate data sharing follows in March 2020.

In addition, the EU Commission has appointed an Expert Group to advise on Business-to-Government Data Sharing (B2G). [54] In its final report, the Expert Group recommends the creation of a recognized data steward function in both public and private sectors, the organization of B2G data-sharing collaborations and the implementation of national governance structures by Member States.[55] The aim of B2G data sharing is to improve public service, deploy evidence-based policy and advise the EU Commission on the development of B2G data sharing policy.

In its 2019 Policy & Investment Recommendations, the High-Level Expert Group on Artificial Intelligence (AI-HLEG) also devoted an entire section to fostering a European data economy, including data sharing recommendations, data infrastructure and data trusts.[56] Finally, in a recent report, the German Opinion of the Data Ethics Commission made 75 authoritative recommendations on general ethical and legal principles concerning the use of data and data technology.

Given that data are generated by such a vast and varied array of devices and activities, and used across so many different economic sectors and industries,

[53] European Commission, ‘A European strategy for data’, Brussels, 19.2.2020 COM(2020) 66 final, https://ec.europa.eu/info/sites/info/files/communication-european-strategy-data-19feb2020_en.pdf & https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_en#documents

[54] Towards a European strategy on business-to-government data sharing for the public interest. Final report prepared by the High-Level Expert Group on Business-to-Government Data Sharing, Brussels, European Union, February 2020, doi:10.2759/731415 https://www.euractiv.com/wp-content/uploads/sites/2/2020/02/B2GDataSharingExpertGroupReport-1.pdf The report provides a detailed overview of B2G data sharing barriers and proposes a comprehensive framework of policy, legal and funding recommendations to enable scalable, responsible and sustainable B2G data sharing for the public interest.

[55] *Ibid*.

[56] High-Level Expert Group on Artificial Intelligence, ‘Policy and Investment Recommendations for Trustworthy AI’ (European Commission, 26 June 2019). https://ec.europa.eu/digital-single-market/en/news/policy-and-investment-recommendations-trustworthy-artificial-intelligence

it is not easy to picture an all-inclusive single policy framework for data.[57]

Dutch vision on B2B data sharing

At the beginning of this year, the Dutch government published a booklet about the Dutch Digitization Strategy, in which it sets out its vision on data sharing between companies. This vision consists of 3 principles:

- Principle 1: Data sharing is preferably voluntary.
- Principle 2: Data sharing is mandatory if necessary.
- Principle 3: People and companies keep a grip on data.

The Dutch Ministry of Economic Affairs is currently exploring the possibilities of encouraging the use of internationally accepted FAIR principles in sharing private data for AI applications. FAIR stands for (Findable, Accessible, Interoperable, Reusable). The Personal Health Train initiative builds on FAIR data principles.[58]

Recent Dutch initiatives in the field of data sharing are the Dutch Data Coalition (self-sovereignty of data), aimed at cross-sectoral data sharing between companies and institutions, the Dutch AI Coalition (NL AIC) as well as some hands-on Data Platform and Data Portal projects from leading academic hospitals, Universities of Technology and frontrunning companies.

5. Mixed datasets: 2 laws (GDPR & FFD Regulation) in tandem

More and more datasets consist of both personal and non-personal machine generated data; both the General Data Protection Regulation (GDPR)[59] and the Regulation on the free flow of non-personal data (FFD)[60] apply to these "mixed datasets". The Commission has drawn up guidelines for these mixed datasets where both the FFD Regulation and the GDPR apply, including its right to data portability.[61] Based on these two Regulations, data can move freely within the European Union.[62]

[57] *Ibid*. (*supra* note 6)

[58] Johan van Soest, Chang Sun, Ole Mussmann, Marco Puts, Bob van den Berg, Alexander Malic, Claudia van Oppen, David Towend, Andre Dekker, Michel Dumontier, ‘Using the Personal Health Train for Automated and Privacy-Preserving Analytics on Vertically Partitioned Data’, Studies in Health Technology and Informatics 2018, 247: 581-585

[59] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). A new European ePrivacy Regulation is currently under negotiation. Data protection and privacy are two different things.

[60] Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union (FFD Regulation).

[61] Practical guidance for businesses on how to process mixed datasets: https://ec.europa.eu/digital-single-market/en/news/practical-guidance-businesses-how-process-mixed-datasets

[62] Besides the GDPR, the Law Enforcement Directive (LED) regulates requirements aimed at ensuring that privacy and personal data are adequately protected during the use of AI-enabled products and services. LED: Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention,

Market barriers for early-stage AI-startups

The GDPR thoroughly protects the personal data of EU citizens. In some cases however, GDPR legislation is also hampering the European internal market with regard to the rapid rollout of AI and data startups (SME's). This applies in particular to a smaller group of early-stage AI-startups who often lack sufficient resources to hire a specialized lawyer or a Data Protection Officer. Therefore, these companies are hesitant to do anything spectacular with personal data, [63] and otherwise in large public-private consortia in which one operates 'gründlich', but where it takes (too) long to create the necessary trust among the participants. This hinders the innovative performance of early-stage AI-startups. In that sense, complex data protection rules do not encourage ambitious moonshot thinking, creative, revolutionary AI and data field experiments and the design of clever products that solve real-world problems. It is paramount that the whole field has a good grasp on the legal dimensions of their data. And that there are no significant restrictions and market barriers in that important early stage.[64] Sharing data is simply a necessary condition for a successful AI ecosystem.[65]

Precautionary principle

A second axiom that has the potential to inhibit rapid scientific advances in the EU - in case of expected large risks or unknown risks- is the precautionary principle. EU lawmakers have a tendency to minimize risk and prevent all possible negative scenarios ex ante via legislation. It doesn't make drafting directives and regulations faster. Rigid application of the precautionary principle in EU law promotes excessive caution and hinders progress. It remains at odds with accelerated technological innovation.[66]

6. California Consumer Privacy Act (CCPA 2020)

The GDPR also has some important advantages for European startups and scaleups. The advantage of the GDPR is that it is now the international standard in the field of the use of personal data when doing business internationally.[67] Partly for this reason, California has largely taken

investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

[63] I speak from personal experience in our law firm. This concerns especially European AI-startups who often do not have the necessary budget to be properly advised on how to navigate data protection and data sharing regulation. See for a first report that confirms this claim: OECD Report 'Enhancing Access to and Sharing of Data - Reconciling Risks and Benefits for Data Re-use across Societies', November 26, 2019, Chapter 4. https://www.oecd.org/sti/enhancing-access-to-and-sharing-of-data-276aaca8-en.htm

[64] A solution that takes away legal roadblocks and encourages market entry of early-stage AI-startups could be targeted government funding in the form of knowledge vouchers.

[65] From this point of view, innovation remains at odds with privacy.

[66] In certain domains, performing independent audits and conformity assessments by notified bodies might be a better option. Especially in a civil law legal tradition, where lawmakers draft concise statutes that are meant to be exhaustive.

[67] With 500 million consumers, Europe is the largest single market in the world.

over the spirit/contents[68] of the GDPR, and implemented it -with a fundamental American approach- in its own regulations that better protect consumer data and safeguard the trade thereof. [69] The California Consumer Privacy Act (CCPA 2020), state-level privacy legislation, came into force on January 1, 2020. [70] If European startups and scaleups are completely GDPR-proof, there will be no privacy legislation anywhere in the world that will require major changes to their personal data protection policy, including the associated legal uncertainty and legal costs. This is a significant competitive advantage. From that lens, European tech startups and AI-scaleups have a head start on their competitors from outside the European Union.[71]

7. Future EU AI and Data Regulation: CAHAI & EU Commission Whitepaper

Transformative technology is not a zero sum game, but a win-win strategy that creates new value. The Fourth Industrial Revolution will create a world where anything imaginable to improve the human condition, could actually be built.[72]

The CAHAI (Ad Hoc Committee on Artificial Intelligence), established by the Committee of Ministers of the Council of Europe[73] is currently examining the possibility of a binding legal framework for the development, design and application of AI and data, based on the universal principles and standards of the Council of Europe on human rights, democracy and the rule of law. The CAHAI expects to be able to report by March 2020 on the possibilities and necessity of new legislation.

Both data sharing practices and AI-Regulation are high on the EU Commission's agenda. On February 19th 2020, the EU Commission published its 'White Paper On Artificial Intelligence - A European approach to excellence and trust'. [74] Fortunately, the White Paper uses a risk-based approach, not a precautionary principle-based approach. The Commission '*supports a regulatory and investment oriented approach with the twin objective of promoting the uptake of AI and of*

[68] For a close comparison of the GDPR and California's privacy law, see Chander, Anupam and Kaminski, Margot E. and McGeveran, William, 'Catalyzing Privacy Law' (August 7, 2019). U of Colorado Law Legal Studies Research Paper No. 19-25. Available at SSRN: https://ssrn.com/abstract=3433922 The article contends that California has emerged as an alternate contender in the race to set the new standard for privacy (which, as mentioned in note 3, is not always the same as data protection).

[69] Mark A. Lemley, 'The Splinternet', Lange Lecture Duke Law School, January 22 2020, https://www.youtube.com/watch?v=5MEl4c5BVCw

[70] https://oag.ca.gov/privacy/ccpa

[71] Such as China, India, Japan, South Korea and Taiwan.

[72] Autonomous AI agents that utilize data and deep learning techniques to continuously perform and improve at its tasks already exist. AI agents that autonomously invent novel technologies and create original art. These AI systems need data to mature.

[73] The Council of Europe, located in Strasbourg, France is not the same governing body as the European Commission. The Council of Europe is not part of the European Union. The European Court of Human Rights, which enforces the ECHR, is part of the Counsel of Europe.

[74] European Commission, White Paper on Artificial Intelligence - A European approach to excellence and trust, Brussels, 19.2.2020 COM(2020) 65 final, https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf

addressing the risks associated with certain uses of this new (data-driven) technology.' [75] In its White Paper, the Commission addresses issues concerning the scope of a future EU regulatory framework and -to ensure inclusiveness and legal certainty- discusses requirements for the use of training datasets.[76] In addition, the Commission contends that independent audits, certification and prior conformity assessments [77] for high risk areas like Health and Transportation, could be entrusted to notified bodies (instead of commercial parties) designated by Member States. The Commission concludes with the desire to become a global hub for data and to restore technological sovereignty.

Pareto optimum

When developing informed transformative tech related policies, the starting point is to identify the desired outcome.[78] In the case of IP policy, that outcome would be to compose a regime that balances underprotection and overprotection of IP rights per economic sector. IP is supposed to serve as a regulatory system of stimulation of creation and innovation that uses market dynamisms to reach this objective.[79] The goal should be no less than a *Pareto optimum* and if possible a *Pareto improvement* by incentivizing innovation, encouraging scientific progress and increasing overall prosperity.[80]

Modalities of AI-regulation

Law is just one modality of AI-regulation.[81] Other important regulatory modalities to balance the societal effects of exponential innovation and digital transformation are the actual design of the AI system, social norms and the market.[82] Data governance should be less fixed on data ownership and more on rules for the usage of data.

The goal should be global open data sharing community with freedom to operate and healthy competition between firms, including unification of data exchange models so that they are interoperable and standardized in the IoT.[83] There is an urgent need for comprehensive, cross sectoral data reuse policies that include

[75] *Ibid*.
[76] *Ibid*.
[77] Alternative Regulatory Instruments (ARIs) such as the AI Impact Assessment, see: https://airecht.nl/blog/2018/ai-impact-assessment-netherlands See also: Carl Vander Maelen, 'From opt-in to obligation? Examining the regulation of globally operating tech companies through alternative regulatory instruments from a material and territorial viewpoint', International Review of Law, Computers & Technology, 2020, DOI: 10.1080/13600869.2020.1733754
[78] See also WIPO (supra note 8). WIPO is comparing the main government instruments and strategies concerning AI and IP regulation and will create a dedicated website that collects these resources for the purpose of information sharing.
[79] Hilty (*supra* note 47)
[80] Kop (*supra* note 40)
[81] Smuha, Nathalie A., From a 'Race to AI' to a 'Race to AI Regulation' - Regulatory Competition for Artificial Intelligence (November 10, 2019). Available at SSRN: https://ssrn.com/abstract=3501410. The author contends that AI applications will necessitate tailored policies on the one hand, and a holistic regulatory approach on the other, with due attention to the interaction of various legal domains that govern AI.
[82] Lawrence Lessig, The Law of the Horse: What Cyberlaw Might Teach, 113 Harvard Law Review 501-549 (1999)
[83] Otero (*supra* note 37). For user generated data see: Shkabatur, Jennifer, 'The Global Commons of Data' (October 9, 2018). Stanford Technology Law Review, Vol. 22, 2019; GigaNet: Global Internet Governance Academic Network, Annual Symposium 2018. Available at SSRN: https://ssrn.com/abstract=3263466

standards for interoperability[84], compatibility, certification and standardization.[85]

Against this background, strengthening and articulation of competition law is more opportune than extending IP rights.[86] Within the context of AI-regulation and data sharing practices, there is no need for adding extra layers of copyrights, database rights, patent rights and trade secret rights.[87]

Technology shapes society, society shapes technology

Society should actively shape technology for good. The alternative is that other societies, with social norms and democratic standards that perhaps differ from our own public values, impose their values on us through the design of their technology.

AI for Good norms, such as data protection by design and by default, as well as Accountability of controllers and processors, transparency, trust and control should be built in the architecture of AI systems and high quality training datasets from the first line of code.[88] In practice, this can be accomplished through technological synergies such as a symbiosis of AI and blockchain technology. Crossovers can offer solutions for challenges concerning the AI-black box, algorithmic bias and unethical use of data.[89] That way, society can benefit from the benevolent side of AI.

Robust, collaborative AI framework development standards such as federated machine leaning[90] models provide personalized AI and safeguard data privacy, data protection, data security and data access rights. Using Privacy by Design as a starting point, with build in public values, the federated learning model is consistent with Human-Centered AI and the European Trustworthy AI paradigm.[91]

[84] For an example of interconnectivity and interoperability of databases in line with the fundamental rights standards enshrined in the EU Charter: Quintel, Teresa, Connecting Personal Data of Third Country Nationals: Interoperability of EU Databases in the Light of the CJEU's Case Law on Data Retention (March 1, 2018). University of Luxembourg Law Working Paper No. 002-2018. Available at SSRN: https://ssrn.com/abstract=3132506

[85] John Wilbanks; & Stephen H Friend, 'First, design for data sharing', (Nature, 2016)

[86] Drexl, (*supra* note 2). The Fourth Industrial Revolution may even require a complete redesign of our current IP regime.

[87] Kop (*supra* note 40). For non-IP policy tools that incentivize innovation, see: Hemel, Daniel Jacob and Ouellette, Lisa Larrimore, 'Innovation Policy Pluralism' (February 18, 2018). Yale Law Journal, Vol. 128, p. 544 (2019); Stanford Public Law Working Paper; Stanford Law and Economics Olin Working Paper No. 516; U of Chicago, Public Law Working Paper No. 664; University of Chicago Coase-Sandor Institute for Law & Economics Research Paper No. 849. Available at SSRN: https://ssrn.com/abstract=3125784. See also: Mauritz Kop, 'Beyond AI & Intellectual Property: Regulating Disruptive Innovation in Europe and the United States – A Comparative Analysis' (December 5 2019) https://law.stanford.edu/projects/beyond-ai-intellectual-property-regulating-disruptive-innovation-in-europe-and-the-united-states-a-comparative-analysis/

[88] Kop (*supra* note 40)

[89] Combination is the key. Examples of potential unethical use of AI are facial recognition and predictive policing.

[90] See note 30 and 31.

[91] High-Level Expert Group on Artificial Intelligence, 'Ethics Guidelines for Trustworthy AI' (European Commission, 8 April 2019). See https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=60419. See also Paul Opitz, 'European Commission Working on Ethical Standards for Artificial Intelligence (AI)', TTLF Newsletter on Transatlantic Antitrust and IPR Developments Stanford-Vienna

As technology shapes society, society shapes technology.

Transatlantic Technology Law Forum, Stanford University, 2018 Volume 3-4, https://ttlfnews.wordpress.com/2018/06/08/european-commission-working-on-ethical-standards-for-artificial-intelligence-ai/

Other developments

European Union

Crypto Regulatory Recommendations of the European Commission's Expert Group on Regulatory Obstacles to Financial Innovation in the EU

By Jonathan Cardenas

In December 2019, the European Commission's Expert Group on Regulatory Obstacles to Financial Innovation ("ROFIEG") published its *Thirty Recommendations on Regulation, Innovation and Finance* report (the "Report"). [92] In its Report, ROFIEG provides the European Commission with a number of regulatory recommendations related to FinTech, including adjustments to the existing EU financial services regulatory framework, the introduction of new regulatory measures in response to FinTech developments, and enhanced cooperation with international standard-setting bodies in order to safeguard the EU's regulatory sovereignty in the FinTech space. This article briefly summarizes ROFIEG's general EU FinTech regulatory recommendations, as well as those specifically related to distributed ledger technology ("DLT") and crypto-assets.

I. ROFIEG Overview

ROFIEG is a group of European legal and financial FinTech experts, led by Professor Philipp Paech of the London School of Economics, that was formed by the European Commission in the spring of 2018 in connection with the launch of the European Commission's FinTech Action Plan.[93] The group was formed to review the applicability of the current EU regulatory regime to FinTech, with an eye to identifying obstacles that could hinder the ability of FinTech companies to scale-up across the EU, as well as those that could impact the competitiveness of the EU in global FinTech markets.

II. General Regulatory Recommendations

a. Regulatory Principles

[92] ROFIEG, 30 Recommendations on Regulation, Innovation and Finance – Final Report to the European Commission (December 13, 2019). Available at: https://ec.europa.eu/info/files/191113-report-expert-group-regulatory-obstacles-financial-innovation_en.

[93] *See* European Commission, FinTech Action Plan: For a more competitive and innovative European financial sector (March 8, 2018). Available at: https://ec.europa.eu/info/publications/180308-action-plan-fintech_en. *See also*, Cardenas, J., The European Commission's FinTech Action Plan and Proposed Regulation on Crowdfunding, TTLF Newsletter on Transatlantic Antitrust and IPR Developments, Stanford–Vienna Transatlantic Technology Law Forum (June 8, 2018). Available at: https://ttlfnews.wordpress.com/2018/06/08/the-european-commissions-fintech-action-plan-and-proposed-regulation-on-crowdfunding/.

The ROFIEG Report provides the European Commission with recommendations on how to create an "accommodative framework" for EU FinTech regulation that allows the EU to balance the potential benefits that can be derived from FinTech against the potential risks that FinTech poses to European market participants and to the European financial system as a whole.[94] ROFIEG defines FinTech as "technology-enabled innovation in the financial sector" that facilitates the provision, development, digitalization and re-engineering of financial products and services in and across financial institutions.[95] ROFIEG's definition of FinTech includes, but is not limited to, five core technologies that are disrupting business models in the financial services industry, including artificial intelligence, DLT, smart contracts, Internet of Things, and quantum computing. The potential benefits of FinTech identified by ROFIEG include the provision of financial services at a lower cost, the development of a broader range of financial services, the opening of certain financial services that previously may have been inaccessible to consumers and businesses, and the inducement of more effective regulatory compliance mechanisms.[96] The potential risks of Fintech, particularly in relation to the provision of financial services, are described by ROFIEG as falling into two categories: traditional financial services risks – such as custody risk, market misconduct, principal-agent risk, settlement risk and systemic risk – that are enhanced by FinTech; and, entirely new risks that have emerged as a result of the introduction of FinTech, including the risk of incomprehensible financial decisions executed by "black box" artificial intelligence algorithms,[97] as well as the risk of unclear legal recourse in the event of loss or theft of crypto-assets.

ROFIEG's approach to accommodative FinTech regulation is based on the principle of "technological neutrality," which endorses the view that FinTech regulation should be "all-encompassing" and not favor or disfavor a particular technology or sector.[98] ROFIEG suggests that producing a regulatory framework that is tailor-made to specific technologies would be inefficient as it would generate regulatory inconsistency and fragmentation. This suggestion builds on the recognition that the benefits of FinTech cannot be fully materialized by the EU at the present time due, in part, to the absence of a clear and harmonized EU FinTech regulatory framework. In this regard, ROFIEG illustrates that having a fragmented and unharmonized set of rules in each EU Member State impedes the ability of emerging EU FinTech startup companies to quickly generate a large pool of customers across the EU's Single Market, particularly in comparison to international competitors in the U.S. and Asia. ROFIEG recognizes, however, that regulatory harmonization alone will not establish a competitive EU FinTech market. Other issues that are beyond the realm of its Report, such as the availability of venture capital, EU taxation rules and international competition, also impact the competitiveness of the EU FinTech market.

Notwithstanding its emphasis on the principle of technological neutrality,

[94] ROFIEG (2019) at 5.
[95] *Id.* at 9, 22.
[96] *Id.* at 10.
[97] *Id.* at 11.
[98] *Id.* at 12.

ROFIEG also recognizes that exceptions are sometimes appropriate in light of the particular risks and opportunities presented by new technological paradigms, which sometimes should be considered when formulating a regulatory approach to those particular risks. As such, and as is discussed in further detail below, ROFIEG has provided the European Commission with a limited number of regulatory recommendations that are specific to artificial intelligence risks, as well as to DLT and crypto-asset risks.

b. Regulatory Recommendations

Building on the principle of technological neutrality, ROFIEG's recommended approach to EU FinTech regulation is "horizontal" and focused on issues that are common to all FinTech market participants, industries and technologies.[99] By identifying themes that cut across the entire FinTech market, ROFIEG suggests that regulatory strategies can be formulated in response to those common themes, which will help to ensure that the EU FinTech regulatory framework is "future-proof."[100] In its report, ROFIEG has identified five common FinTech themes for which it has formulated regulatory strategies: understanding technology and its impact; cyber resilience; outsourcing; governance of distributed financial networks (including crypto-assets); and standardization, RegTech and SupTech.

ROFIEG's thirty regulatory recommendations can be broken down into four general categories: (1) the need to adapt existing regulation and/or create new regulation that is "fit for purpose" with respect to both modified forms of traditional financial risk as well as new forms of financial risk created by FinTech,[101] (2) the need to adopt harmonized regulation based on the "similar activity, similar risk, same rule" principle in order to capture new financial services that fall outside of the scope of current EU law,[102] (3) the need to reconcile European data protection regulation with FinTech-related data risks and opportunities, and (4) the need to consider the potential societal impacts of FinTech on issues of financial inclusion/exclusion and unfair discrimination.

III. Crypto Regulatory Recommendations

a. Overview

Mindful of the lack of uniformity that presently exists worldwide in the conceptualization of DLT and blockchain technology ("blockchain"), ROFIEG uses the following definitions for purposes of its Report. DLT is defined as an umbrella term for "multi-party systems that operate in a secure environment with no central operator or authority in place, but which mitigates the risks posed by parties who may be unreliable or malicious."[103] Building on the conceptual work undertaken by the Cambridge Centre for Alternative Finance,[104] blockchain is

[99] *Id.* at 26.
[100] *Id.* at 38.
[101] *Id.* at 38.
[102] This principle stands for the notion that new activities that create risks similar to risks that are covered by existing regulation should be governed by those same rules rather than by newly devised rules targeted specifically to the new activities.
[103] ROFIEG (2019) at 31.
[104] *See also* Rauchs, M. *et al*, 2nd Global Enterprise Blockchain Benchmarking Study, The Cambridge Centre for Alternative Finance, University of Cambridge Judge Business

defined as a "specific subset of the broader DLT universe" that is architecturally based on a "chain of hash-linked blocks of data" that is "distributed over a decentralized peer-to-peer computer network, in which every network node maintains the latest version of the chain of blocks."[105]

ROFIEG recognizes that DLT and blockchain can have applications in financial markets, including, for example, in the areas of payments, digital identity verification and regulatory reporting, as well as in areas as wide ranging and unrelated to financial markets as healthcare and supply chain management. As a result, ROFIEG suggests that DLT and blockchain need not be subject to financial services regulation *per se*. When and if, however, DLT and/or blockchain are used by financial market participants to engage in financial services activities that do fall within the scope of existing financial regulation, financial regulation must also apply to those activities unambiguously.

ROFIEG refers to blockchain networks in which financial services functions are executed as "distributed financial networks."[106] In this regard, crypto-assets, which ROFIEG defines as "entitlements enshrined in a piece of computer code,"[107] are typically stored and transacted on using distributed financial networks. Complex legal questions arise in this setting as the law that applies to distributed financial networks, as well as to crypto-assets that are stored and transacted on using these networks, is presently unclear. In some cases, distributed financial networks and crypto-assets might fall clearly within the realm of existing regulation, while in other cases, existing regulation either does not apply or its application is uncertain. As such, ROFIEG recommends that the European Commission clarify the regulatory framework applicable to distributed financial networks and crypto assets in the following ways.

b. Governance of Distributed Financial Networks

i) Relationships Between Market Participants

As a result of the increased adoption of decentralized financial services, ROFIEG has observed a shift in financial markets from the traditional model of bilateral relationships between financial market participants to a multilateral relationship model. The current EU regulatory framework is built on the traditional bilateral understanding of financial market relationships. As such, when and where financial services are delivered in a distributed financial network setting, the current EU regulatory framework will not necessarily apply since the current rules were not designed for multilateral relationships. This becomes a matter of

School (2019). Available at: https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/alternative-finance/downloads/2019-ccaf-second-global-enterprise-blockchain-report.pdf. *See also* Rauchs, M. *et al*, Distributed Ledger Technology Systems: A Conceptual Framework, The Cambridge Centre for Alternative Finance, University of Cambridge Judge Business School (2018). Available at: https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/alternative-finance/downloads/2018-10-26-conceptualising-dlt-systems.pdf.

[105] ROFIEG (2019) at 32.

[106] *Id.* at 38.

[107] *Id.* at 47.

legal concern particularly with regard to whether or not market participants that interact in a distributed financial network with parties located outside of the EU will have access to legal recourse in the EU or elsewhere. In other words, it is presently unclear how disputes between parties will be settled in a multilateral relationship-driven distributed financial network. As such, there is a need for regulatory clarification in this regard to provide market participants with clarity as to their rights in the distributed financial network context.

ii) Applicability of Established Concepts

In order for EU financial regulation to apply to distributed financial networks, the distributed network(s) in question need(s) to fall within the "perimeter" of EU financial regulation.[108] Where a regulated financial institution starts to utilize distributed financial networks to deploy services in the ordinary course of its business, for example, these uses may fall within the scope of existing EU financial regulation as a result of the type of financial data that is stored on the distributed financial network. Concepts that have been established in existing regulation (including concepts related to accounts, client protection and settlement) may not apply, however, where they were formulated on the basis of the traditional bilateral view of relationships in financial markets. In these cases, preexisting regulatory concepts will need to be adapted to the multilateral distributed financial network context in order to remain relevant.

iii) Addressees of Regulation

Recognizing that the Internet is the underlying operational infrastructure for distributed financial networks and that network participants can operate from anywhere in the world, ROFIEG recommends that a revised EU FinTech regulatory framework clearly define the addressee(s) of such regulation.

iv) Operational Resilience

The increased use of DLT requires that strong uniform operational standards, including cybersecurity standards, be adopted in order to ensure operational resilience and minimize cybersecurity vulnerabilities. In the blockchain context, common standards regulating the management and security of public/private key encryption mechanisms are vital as there may be no recourse for the recovery of lost assets if a private key is lost or stolen. Adopting and applying established best practices can help to minimize the risk of private key loss and overall operational vulnerability.

c. Legal Framework for Crypto-Assets

ROFIEG recommends that the European Commission accelerate its current work in assessing the suitability of existing EU rules to crypto-assets and to implement legislation where necessary to address the risks that flow crypto-asset activities.

i) Harmonized Crypto-Asset Taxonomy

As ROFIEG recognizes, a standardized

[108] *Id.* at 50.

taxonomy for crypto-assets has not yet been developed by the EU nor by international standard-setting bodies. In the crypto-asset context, ROFIEG recognizes that attempts have been made to create a distinction between three presumed categories of crypto assets, namely, exchange tokens, security tokens and utility tokens.[109] ROFIEG, however, does not adopt these distinctions in its analysis as it explains that it takes a "functional view" of the risks and opportunities arising from all forms of FinTech, including those arising from crypto-assets. [110] ROFIEG instead supports the notion that crypto-assets should be analyzed on a "case-by-case basis" and recommends that a "substance-over-form approach" be taken through the lens of existing definitions under EU law.[111]

ROFIEG is of the view that a harmonized regulatory approach to crypto-assets that is built upon the existing EU financial services *acquis communautaire* is necessary in order to avoid a fragmented EU crypto-asset market. ROFIEG agrees with the views expressed by the European Banking Authority ("EBA") and European Securities and Markets Authority ("ESMA") in January 2019 that some crypto-assets may qualify as electronic money or as financial instruments under current EU financial services regulation, while some may fall outside of the scope of EU law.[112] As such, ROFIEG recommends that the European Commission take action to determine whether or not regulatory changes are required in order to address those crypto-assets that currently fall outside of the scope of EU law.

ROFIEG also recognizes that certain EU Member States have adopted their own regulatory measures in an attempt to address crypto-asset risk, including the French Action Plan for Business Growth and Transformation (*Le Plan d'Action pour la Croissance et la Transformation des Entreprises*), [113] the Liechtenstein Token and Trustworthy Technology Service Provider Act (*Token- und VT-Dienstleister-Gesetz*), [114] and the UK Jurisdiction Taskforce's "Legal Statement on the Status of Cryptoassets and Smart Contracts" (published prior to the UK's departure from the EU on January 31, 2020).[115] However, ROFIEG is of the view that national legislation only provides an isolated solution to the regulatory challenges facing the EU at large. It is of the view that diverging regulatory approaches at the EU Member State level create uncertainty for market participants, increase the risk of regulatory arbitrage and impede the ability of firms offering crypto-asset-related

[109] *Id.* at 53.
[110] *Id.* at 54.
[111] *Id.* at 54.
[112] EBA, Report with Advice for the European Commission on Crypto-Assets (2019). Available at: https://eba.europa.eu/sites/default/documents/files/documents/10180/2545547/67493daa-85a8-4429-aa91-e9a5ed880684/EBA%20Report%20on%20crypto%20assets.pdf. ESMA, Advice: Initial Coin Offerings and Crypto-Assets (2019). Available at: https://www.esma.europa.eu/sites/default/files/library/esma50-157-1391_crypto_advice.pdf.
[113] Available at: https://www.gouvernement.fr/action/pacte-le-plan-d-action-pour-la-croissance-et-la-transformation-des-entreprises.
[114] Available at: https://bua.regierung.li/BuA/default.aspx?nr=54&year=2019&erweitert=true.
[115] Available at: https://www.judiciary.uk/announcements/the-chancellor-of-the-high-court-sir-geoffrey-vos-launches-legal-statement-on-the-status-of-cryptoassets-and-smart-contracts/.

services to scale up across the EU market. As such, a harmonized approach at the EU level is needed to avoid this outcome.

ii) Regulation of Crypto-Asset Risk

ROFIEG describes crypto-asset risk as including money laundering and terrorist financing risk, systemic risk posed by regulated financial institution exposure to crypto-assets, client asset protection risk, and pegging and foreign exchange conversion risk associated with crypto-assets that are backed by traditional financial assets. In this regard, ROFIEG again recommends that the EU's regulatory approach follow the "similar activity, similar risk, same rule" principle, thereby avoiding regulatory fragmentation and regulatory arbitrage.

d. Commercial Law of Crypto-Assets

In order to protect the rights of market participants in distributed financial networks, ROFIEG recommends that the European Commission consider whether certain commercial law rules should be made applicable to crypto-assets at the EU level. The application of traditional commercial law doctrines to crypto-assets is presently uncertain at the EU level due, in part, to the various iterations of EU Member State law on the topic. While ROFIEG is of the view that a fully harmonized, EU-wide commercial law framework applicable to crypto-assets would be "difficult to establish and probably neither necessary nor desirable,"[116] it does recommend that clear property law rules regarding ownership of crypto-assets be implemented at the EU level in order to facilitate the creation of a legally protected crypto-asset market across the EU.

ROFIEG also recommends that the European Commission legislate a conflict-of-laws rule for crypto-assets. ROFIEG is of the opinion that a uniform EU crypto-asset conflict of laws rule is needed in order to determine which law applies to crypto-assets that are stored and transacted on using distributed financial networks. An EU crypto-asset conflict of laws rule would allow EU financial market participants to know *ex ante* which law would apply to their crypto-assets and would allow these parties to draft legal agreements with predictability.

[116] ROFIEG (2019) at 59.

Other developments

European Union

An Overview of the EDPB Guidelines on Processing of Personal Data through Video Devices

By Elif Kiesow Cortez

The European Data Protection Board adopted on the 29th January 2020 the guidelines on processing of personal data through video devices. The European Data Protection Board (EDPB) replaced the Working Party 29 established by Directive 95/46/EC [117] and ensures the consistent application of the GDPR[118]. Therefore, the guidelines issued by the EDPB serves as a source to get insights on GDPR compliant practices in processing of personal data through video devices.

Applicability

Scholarly discussions in personal data protection gave special attention to processing of such data collected through video devices [119] . Under the GDPR personal data refers to any information relating to an identified or identifiable natural person. The guidelines highlight that the frequent use of systematic automated monitoring of areas by audio-visual means increases the possibility of identifying the data subjects that use the monitored areas[120].

In the guidelines, the EDPB first defines the scope of applicability of the GDPR by demonstrating possible scenarios. For example, it is discussed that someone filming their holiday on their personal device or using an action camera attached to their sports equipment might fall under the household exemption of the GDPR Article 2 (2) (c) even if this might mean other individuals have been recorded in the background. However, there is specific emphasis that the exemption applies to cases where the recording is shown to friends and family. The guidelines refer to a 2003 decision of the European Court of Justice[121] where it is stating that uploading the video on the internet and making the data available “to an indefinite number of people” would not benefit from household exemption.

[117] EU Directive 95/46: Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ 1995 L 281/31.

[118] EU General Data Protection Regulation (GDPR): Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1.

[119] Ringrose, K. (2019). Law Enforcement's Pairing of Facial Recognition Technology with Body-Worn Cameras Escalates Privacy Concerns. Virginia Law Review Online, 105, 57.

[120] European Data Protection Board Guidelines 3/2019 on processing of personal data through video devices, Version 2.0, adopted on 29 January 2020, p.7.

[121] European Court of Justice, Judgment in Case C-101/01, Bodil Lindqvist case, 6th November 2003, para 47.

Lawfulness

Purpose specification is one of the principles of personal data processing under the GDPR Article 5 (b). Regarding processing of personal data through surveillance cameras, the EDPB asserts that the purpose of the monitoring should be specified and documented for each surveillance camera. It is also explained in the guidelines that "video surveillance for safety" on its own would not be seen as a sufficiently specific purpose. It is further stated that according to Article 6 (1) (c), an exception would be in cases where national law demands as an obligation to monitor through video surveillance.

The guidelines demonstrate an example on when a shop owner could install a video surveillance system. In this example, it is assumed that there is no national law demanding this action and that the shop owner would like to use the "legitimate interest" ground under the GDPR Article 6 (1) (f) as the legal basis for the processing. It is stated that if the shop owner would claim that there is legitimate interest in installing the system to avoid vandalism, then the shop owner is burdened with proving that there are statistics that show that vandalism is an actual threat in the relevant neighborhood (and that it would not be sufficient if this threat exists nationally but does not apply locally to the relevant neighborhood)[122]. It is though stated that imminent danger situations may be seen as legitimate interest ground for shops such as banks or jewelers therefore it can be seen that in these cases neighborhood-specific risk justification might not be required

.

Reasonable Expectation of Privacy

The guidelines state that it is mandatory for data controllers to balance the interests and the fundamental rights of the data subjects and their legitimate interests. The EDPB list some of the balancing factors as the size of the area that is under video surveillance, type of information that is gathered and the amount of data subjects. According to Recital 47 of the GDPR, when data subjects do not reasonably expect their data to be processed, it is likely that the interests and fundamental rights of the data subject would override the interests of the data controller.

The guidelines emphasize that data subjects could reasonably expect that they are monitored by video surveillance at a bank or ATM but they would not be reasonably expecting video surveillance in areas such as their private garden, in fitness facilities, in publicly accessible areas dedicated to regeneration or leisure. The EDPB guidelines also state that signs that inform the data subjects of video surveillance are not relevant in objectively assessing what reasonable expectation of privacy the data subjects might have. In other words, if the monitored area falls within an area where the data subjects have a reasonable expectation of privacy, it cannot be claimed that this expectation is not objectively reasonable only based on the fact that there were signs informing the

[122] European Data Protection Board Guidelines 3/2019 on processing of personal data through video devices, Version 2.0, adopted on 29 January 2020, pp.9-10.

data subject that the area is under video surveillance.

Consent is one of the legal bases for processing an individual's personal data. When it comes to video surveillance, relying on consent as the legal basis of processing might pose problems for the controller given that consent must be collected from every data subject who enters the area that is under video surveillance. Simply entering a marked area would not constitute as valid consent on its own unless it is compliant with the criteria of Article 4 and 7.

Special Categories of Data

It might be possible that a video surveillance recording shows that someone is using a wheelchair. According to GDPR Article 9, this could be seen as health data and therefore fall under special categories of data (sensitive data) however, the EDPB guidelines highlight that video footage showing health circumstances are not always considered to be sensitive data. The guidelines use the following examples that a hospital monitoring a patient's health condition through video camera or using video surveillance in a manner to detect someone's political opinion (i.e. engaging in a strike) would constitute processing of sensitive data however video footage showing that someone uses a wheelchair is not per se considered as processing of sensitive data.

Some examples from the guidelines include a hotel using video surveillance to recognize automatically if a VIP guest is in the hotel premises. In this event, as the face recognition technology would be scanning every guest, explicit consent of every guest must be acquired before the processing. However, in a different example, the EDPB highlights that if a shop would be scanning customers only to detect gender and age of the customers, as this type of processing might not be seen as processing sensitive data if the system does not generate biometric templates of the data subjects.

Concluding remarks

The European Data Protection Board guidelines on processing of personal data through video devices provide several examples on ensuring GDPR compliance with data processing principles and with data subject's rights regarding the use of video devices. This overview of the guidelines shows that additional measures and restrictions might become applicable in the short run for video surveillance practices. Some new measures suggested in the guidelines include that data subject's rights and retention period of the data should be communicated publicly via the informative signs on video surveillance. The guidelines also include a list of organizational and technical measures to assist GDPR compliance. As the use of face recognition technologies becomes more frequent for the use of law enforcement [123] or for targeted advertis-

[123] Satariano, A., Police Use of Facial Recognition Is Accepted by British Court, The New York Times, 4 September, 2019, available at https://www.nytimes.com/2019/09/04/business/facial-recognition-uk-court.html

ing[124], the guidelines would serve to achieve a more uniform approach on processing of personal data through video devices within the EU.

[124] Kuligowski, K., Facial Recognition Advertising: The New Way to Target Ads at Consumers, Business News Daily, July 18, 2019, available at https://www.businessnewsdaily.com/15213-walgreens-facial-recognition.html & Lewinski, P., Trzaskowski, J., & Luzak, J. (2016). Face and emotion recognition on commercial property under EU data protection law. Psychology & Marketing, 33(9), 729-746.

Other developments

European Union

Data Snooping and the UK Class action against Google

By Odysseas G. Repousis

In October last year, the UK Court of Appeal overturned the English High Court's prior block on a class action lawsuit brought on behalf of four million iPhone users against Google. The claims arise out of the notorious 'Safari Workaround', which, for several months in 2011 and 2012, allegedly allowed Google to track cookies on Apple handset devices without the user's knowledge or consent.[125]

Whilst the Court of Appeal's judgment is not the end of it, as it merely means that the case may now proceed to the merits, it is nonetheless a ground-breaking ruling that sets a precedent for similar privacy cases and also tests the limits of data privacy class actions in the UK and beyond.

Background

The UK class action has its genesis on the discovery in early 2012 of the 'Safari Workaround', and the subsequent regulatory action that was taken against Google by the Federal Trade Commission (FTC).[126]

Unlike most other internet browsers, Apple's Safari, was set by default to block third party cookies (*i.e.* data sent from websites or domains recording the user's browsing activity). There were however certain exceptions to these default settings, which were in place until March 2012, when the software was updated. Therefore between 2011 and March 2012, those exceptions allegedly enabled Google to access iPhone users' Safari browsing history without their knowledge or consent.[127] This reportedly enabled Google to collect information "as to the order in which and the frequency with which websites were visited … users' internet surfing habits and location, but also [information] about such diverse factors as their interests and habits, race or ethnicity, social class, political or religious views or affiliations, age, health, gender, sexuality, and financial position".[128] In turn, Google would allegedly offer the data it had collected to subscribing advertisers.[129] This is what came to be known as the 'Safari Workaround'.

In August 2012, Google agreed to pay a US$22.5 million civil penalty to settle charges brought by the FTC.[130] The basis

[125] Jane Wakefield, *Google faces mass legal action in UK over data snooping*, Nov. 30, 2017, https://www.bbc.co.uk/news/technology-42166089.

[126] *Richard Lloyd v Google LLC* [2018] EWHC 2599 (QB), Judgment, Oct. 8, 2018, para. 13 (Noting that "Google's activities in relation to the Safari Workaround were discovered by a PhD researcher, Jonathan Mayer … and publicised in blog posts and, on 17 February 2012, in the Wall Street Journal").

[127] [2018] EWHC 2599 (QB), paras. 8-19.

[128] *Ibid.*, para. 11.

[129] *Id.*

[130] FTC, Google Will Pay $22.5 Million to Settle FTC Charges it Misrepresented Privacy Assurances to Users of Apple's Safari Internet Browser, Aug. 9, 2012,

for the penalty was that Google had misrepresented to Safari users that it would not track their browsing activity by placing tracking cookies and would not serve targeted advertisements to those users.[131] On 11 November 2013, Google also agreed to pay US$17 million to settle consumer-based actions brought against it by attorneys general representing 37 US states and the District of Columbia.[132] Several class actions were also filed in the US and were later consolidated. In 2016, Google agreed to settle those by paying US$5.5 million to educational institutions or non-profits organisations (however, the terms of this settlement remain in dispute).[133]

The first UK claim was filed in June 2013 by three individuals.[134] In that case, which is known as the *Vidal-Hall* case, the claimants claimed damages for *distress* as a result of Google's breaches of the UK Data Protection Act1998 (**Data Protection Act**). That claim was allowed, and Google's appeal was dismissed.[135]

The UK class action was filed in May 2017. This class action is brought by Richard Lloyd, a former director of consumer group *Which?*, on behalf of four million UK iPhone users, who were allegedly affected by the 'Safari Workaround'. Specifically, the allegation is that by bypassing the privacy settings on Apple handsets, Google gathered personal data, and used that data for targeted advertising without the users' consent. The class action is therefore a claim for damages for the loss of control over personal data.

Whilst the factual matrix of the UK class action and of *Vidal-Hall* is similar, there is one crucial difference between the two actions: in *Vidal-Hall*, the three individual claimants claimed damages for *distress* as a result of Google's breaches of the DPA. In the class action, the class representative, Mr. Lloyd, claimed "a uniform amount by way of damages on behalf of each person within the defined class without seeking to allege or prove any distinctive facts affecting any of them, save that they did not consent to the abstraction of their data".[136] That amount has yet to be fully quantified but could reportedly be as high as £750 for each class member.[137]

A key question that was therefore at issue was whether, as a matter of UK law, a claim for a tariff award was improper in circumstances where the facts and damages pleaded in the class action were not individualized.

https://www.ftc.gov/news-events/press-releases/2012/08/google-will-pay-225-million-settle-ftc-charges-it-misrepresented.

[131] [2018] EWHC 2599 (QB), para. 13.

[132] *Richard Lloyd v Google LLC* [2018] EWHC 2599 (QB), Judgment, Oct. 8, 2018, para. 13 (Noting that "Google's activities in relation to the Safari Workaround were discovered by a PhD researcher, Jonathan Mayer … and publicised in blog posts and, on 17 February 2012, in the Wall Street Journal").

[133] The Google Cookie Class Action Lawsuit is In re: Google Inc. Cookie Placement Consumer Privacy Litigation, Case No. 17-1480, in the U.S. Court of Appeals for the Third Circuit; https://topclassactions.com/lawsuit-settlements/privacy/912971-5-5m-google-cookie-class-action-settlement-tossed-3rd-circ/

[134] *Vidal-Hall v Google Inc* [2014] EWHC 13 (QB), Judgment, Jan. 16, 2014, para. 5.

[135] *Google Inc v Vidal-Hall* [2015] EWCA Civ 311, Judgment, Mar. 27, 2015.

[136] *Richard Lloyd v Google LLC* [2018] EWHC 2599 (QB), Judgment, Oct. 8, 2018, para. 3.

[137] *Id.*

First instance: No claim for damages without individualized proof of loss or distress

In deciding the matter, the English High Court (per Warby J), determined that the members of the class had failed to show that they suffered 'damage' as a result of Google's infringement of the Data Protection Act. Specifically, section 13 of the Data Protection Act provided that "[a]n individual who suffers damage by reason of any contravention by a data controller of any of the requirements of this Act is entitled to compensation from the data controller for that damage".[138] The "real and substantial issue between the parties" was therefore "whether the impact of the Safari Workaround on the Representative Claimant and the other Class members" amounted to 'damage' within the meaning of the Data Protection Act.[139] In *Vidal-Hall*, the Court of Appeal had determined that non-material damage, in the form of distress and anxiety, fell within the scope of section 13 of the Data Protection Act.[140] However, the class action did not depend upon "any identifiable individual characteristics of any of the claimants, or any individual experiences of or concerning the Safari Workaround" and there was "no allegation that any individual suffered any distress or anxiety, however slight".[141] In other words, the question was whether the class representative (and the individual members of the class) could bring a claim for damages "on a uniform per capita basis" without proof or particularization of pecuniary loss, distress, anxiety, embarrassment, or any other individualized allegation of harm.[142]

The High Court answered this question in the negative holding that the claim did not disclose a basis for seeking compensation under the Data Protection Act.[143] In the alternative, the High Court held that the class action ought to be dismissed because the members of the class did not have the "same interest" and/or it could not be supposed that the breach of duty or the impact of it was uniform across all members of the class.[144] In the further alternative, the High Court determined that the action should not be allowed to continue as a matter of discretion because it would have been very difficult to verify the affected members of the class, and there was "an obvious risk" that compensation would go to persons who did not suffer damage.[145] Therefore, in the High Court's view, the class action ought not be allowed to "consume substantial resources in the pursuit of litigation on behalf of others who have little to gain from it, and have not authorised the pursuit of the claim, nor indicated any concern about the matters to be litigated".[146]

Appeal: Loss of control over personal data is compensable even absent proof of loss or distress

The main issue that was raised on appeal was whether the English High Court was right to hold that the members of the class

[138] *Ibid*., para. 26.
[139] *Ibid*., para. 48.
[140] *Ibid*., para. 49.
[141] *Ibid*., para. 26.
[142] *Ibid*., para. 23.
[143] *Ibid*., paras. 54-81.
[144] *Ibid*., paras. 82-105.
[145] *Ibid*., para. 95.
[146] *Ibid*., para. 104.

could not recover uniform per capita damages for the infringement of their data protection rights without proving pecuniary loss or distress.[147] Delivering the opinion of the Court, Voss LJ held that "key to these claims" was "the characterisation of the class members' loss as the loss of control or loss of autonomy over their personal data".[148] And even if personal data is not technically regarded as property in English law, it is clear that browser generated information has economic value: it can be collected and sold to advertisers who wish to target individual consumers with their advertising. [149] This "confirms that such data, and consent to its use, has an economic value". [150] On that basis, the Court of Appeal held that damages could in principle be awarded for loss of control of data even if there was no proof of pecuniary loss or distress.

Once it was determined that the members of the class all had something of value – their browser generated information – taken from them without their knowledge or consent, the matter of commonality was more straightforward. In the words of the Court of Appeal, the "class are all victims of the same alleged wrong, and have all sustained the same loss, namely loss of control over their" browser generated information. [151] That the members of the class sought to recover uniform per capita damages did not mean that they did not have the "same interest". Rather, as the Court of Appeal explained, "[i]f individual circumstances are disavowed", – as was the case here – the class representative "could, be entitled to claim a uniform sum in respect of the loss of control of data sustained by each member of the represented class".[152] That sum would "be much less than it might be if individual circumstances were taken into account, but it will not be nothing" – it is merely the lowest common denominator.[153] The Court of Appeal was therefore convinced that the members of the class had the "same interest" and were identifiable. As to the matter of discretion, the Court of Appeal held that the class action was the only way in which these claims could be pursued. It would therefore be wholly disproportionate to block the action on the basis that it would be costly and would use up the English Court's valuable resources. Such a result would leave the members of the class without a remedy.[154]

In light of the above, the Court of Appeal overturned the High Court judgment and allowed the case to proceed to the merits.

Concluding remarks: What lies ahead?

The Court of Appeal's judgment in *Richard Lloyd v Google LLC* is no doubt a milestone in data privacy actions. It clarifies the law applicable to class actions pursued on the basis of alleged data protection violations. It also sheds light on the heads of compensable damage for serious infringements of data protection laws.

Most importantly, this judgment comes at a time when the full scope, extent and application of the EU's General Data

[147] *Richard Lloyd v Google LLC* [2019] EWCA Civ 1599, Judgment, Oct. 2, 2019, para. 4.
[148] *Ibid*., para. 45.
[149] *Ibid.*, para. 46.
[150] *Id*.
[151] *Ibid*., para. 75.
[152] *Ibid*., para. 77.
[153] *Id*.
[154] *Ibid*., para. 86.

Protection Regulation (GDPR) and the UK's Data Protection Act 2018 (which complements the GDPR's application in the UK and updates the Data Protection Act 1998) remain to a large extent uncharted. And whilst it is highly likely that the Court of Appeal's judgment will be of important precedential value, it remains to be seen to what extent it will influence similar actions under the GDPR. Suffice it to note that the GDPR itself, in somewhat promethean manner, provides that "non-material damage" includes "loss of control over personal data".[155]

[155] *See* GDPR, Recital 85 and Art. 82.1. The Court of Appeal found this "helpful although not decisive". *See* [2019] EWCA Civ 1599, paras. 64-65.