European Intellectual Property Review

A journal concerning the management of technology, copyrights and trade names

OPINION
Creative Machines: Ownership of Copyright in Content Created by Artificial Intelligence Applications
Julia Dickenson, Alex Morgan and Birgit Clark

ARTICLES
Let’s Talk about Data Ownership
Anette Gärtner and Kate Brimsted
The Mark of a Culture: The Efficacy and Propriety of Using Trade Mark Law to Deter Cultural Appropriation: Part 2: Practical Consequences and Legal Hurdles
Sari Sharoni
Rethinking Hyperlinking: Addressing Hyperlinking to Unauthorised Content in Copyright Law and Policy
Jorinde Mielke
Developments Regarding the Patentability of Computer Implemented Inventions within the EU and the US: Part 1—Introduction and the Legal Problem of Patenting Computer-Implemented Inventions
Dr Sinan Utku and Professor Alain Strowel

COMMENTS
Laches and Statutes of Limitations in Patent Infringement Actions: The US Supreme Court Reaffirms Petrella
Stefano Barazza
Humira Patent Rights Shot by "Fujifilm declaration"
Dr Manuel Kunst and Dr Janet Strath
Fragile Opponent Outcome Trends in Japanese Patent Oppositions
John A. Tessensohn

BOOK REVIEWS

SWEET & MAXWELL
Let’s Talk about Data Ownership

Anette Gärtner
Reed Smith LLP

Kate Brimsted
Berwin Leighton Paisner LLP

Comparative law; Confidential information; Copyright works; Data; EU law; Germany; Ownership; Personal property; Trade secrets

As personal devices, vehicles and industrial control systems increasingly join the ranks of the Internet of Things, the volume and potential value of big data rise exponentially. Private and public stakeholders are certainly focusing on the possibilities of “data” as never before. But if data are really the new “oil”, then is the current legal framework fit for purpose? Does it provide adequate certainty over the ownership and licensing of this burgeoning commodity? And what are the implications of data protection law? Against the background of a current European Commission consultation and the imminent arrival of the GDPR, this article explores these questions from a civil and a common law perspective.

You hear the buzzwords every day: big data, connected cars, the Internet of Things. Many of us take for granted that cars are not merely a means of transportation but rather are powerful computers on wheels, analysing mechanical performance (and that of the driver) as well as sampling the environment and interfacing with its user, not to mention the manufacturers of the vehicle and its sub-systems. Thanks to sensors in everyday devices, most of us are leaving a wide digital data exhaust in our wake.

For industry, governments and lawyers, this inevitably raises questions such as: What kind of legal framework do we need to support the digital economy? Should that include a separate, discrete “data ownership” right? If so, how do we delineate that and who should own it? Since 2012 these questions have been at the heart of one of the biggest legal debates in Germany. The European Commission also recently identified “ownership, access and trade in digital data” as a hot topic in the context of the Digital Single Market and has issued a series of related papers.2

Against this background, this article considers the current law in relation to data ownership from a civil (German) and common law (English) perspective. It also briefly explores whether there is an economic rationale for creating a right to data, before illustrating how data protection law adds another layer of complexity. This article concludes with the authors’ view that the case for a new data property right appears as yet unproven.

Is there such as thing as data ownership?

There are various aspects to this question. In the following sections, we will explain why copyright law is of limited relevance in this context, before addressing the circumstances under which data are protected as confidential information. This leads to a broader discussion of “data as property” that also references criminal law.

Data, copyright and database right

Despite all doctrinal differences, neither German nor English copyright law protects data “as such”. An email may have the required level of originality to qualify as an author’s work, but machine-generated data will generally be lacking the human creativity component. If data are arranged in a systematic way, and are accessible by electronic means, the special protection for databases kicks in. Having said this, the sui generis rights of the database owner only relate to the database, not the individual elements.3 For an analysis of data ownership, copyright law is thus of limited relevance.

Data as confidential information

Data may, however, be protected as confidential information. For the purposes of this discussion, we will examine two different scenarios: in the first one we are looking at a production facility monitored by a computer system which collects and analyses measurement data on a continuing basis. The purpose in doing this is to ensure that the sources of any malfunctions can be swiftly identified. The measurement data are not transmitted to any third parties.

1 Dr Anette Gärtner, LLM (Edinburgh), Rechtsanwalt and Solicitor, Frankfurt; Kate Brimsted, MEng & Man, . The authors would like to thank Ms Ann-Christine Tröbs, LLM (Glasgow) for her kind research assistance.
2 Herbert Zach, Information als Schutzgegenstand (Tübingen: Mohr Siebeck, 2012).
In the second scenario, we consider a connected or “networked” car. While that car cannot yet drive without a human being behind the steering wheel, it features assistance systems that help the driver park his vehicle and that automatically engage the brakes in situations of danger, such as a pedestrian suddenly crossing the road. In addition, garages authorised to service the vehicle rely on the data saved by the “black box” when the car requires repair. Those data are also transmitted to and used by the car manufacturer for future product development.

German Act on Unfair Competition (UWG)

Do the rules on trade secret protection provide relief if either of these data types is passed on to a third party? In the absence of relevant case law, the cautious German lawyer will answer: it depends. Section 17 UWG protects the “owner” of a trade secret against certain acts that are considered unfair. An example of this would be where an employee communicates a trade secret, to which he has access during his employment, to a third party. A breach of s.17 UWG results in criminal liability, as well as giving rise to a cease and desist claim and liability for damages (ss.8(1), 9 UWG).

For s.17 UWG to come into play, the information at issue must be a trade secret. According to case law, this implies that (1) the information must be secret, and (2) that it must be attributable to a company. In the first scenario, it could be argued that the measurement data are secret because they are not intended to be transmitted to third parties. One can further take the view that the data can be attributed to the company that runs the production facility, because this company has the data measured and stored on its computer system. There is thus good reason to argue that the data constitute trade secrets in terms of s.17 UWG.

In the second scenario, by contrast, it is far less clear whether or not the data falls within the scope of s.17 UWG. Depending on how many people have access to the data and whether they are bound by confidentiality agreements, it is questionable whether the information is (still) secret. In addition, it appears rather difficult to attribute the data to an individual company and its business. Several companies, i.e. the car manufacturer, the supplier of the assistance systems as well as all authorised garages, use the data for a multitude of purposes. Which of these companies—if any—may legitimately be considered the “owner”?

On a more general note, one must not forget that s.17 UWG is a criminal law provision and thus interpreted narrowly. It only covers the unfair activities expressly mentioned in s.17 UWG. For example, a former employee who communicates a trade secret to a third party after the end of his employment does not breach s.17(1), and depending on the circumstances of the individual case may not be liable pursuant to s.17(2) UWG either. In contrast to, e.g., patented inventions that enjoy protection against any act of infringement, the UWG merely sanctions certain types of unfair conduct. It does not recognise data ownership as a distinct right.

Equity

Under English law, the situation is not that dissimilar. Equity provides protection to information that is merely confidential and non-trivial, as well as to trade secrets. The distinction between these two categories is relevant for the level of protection. An employee must not disclose confidential information to a third party during the term of his employment. Trade secrets, by contrast, also enjoy protection after the termination of the employment. According to Lansing Linde Ltd v Kerr, a piece of information constitutes a trade secret if the following requirements are met:

- if it is used in trade or business;
- if disclosed to a competitor, it would be liable to cause real or significant damage to the owner of the secret;
- if the owner has sought to limit dissemination.

With regard to the scenarios described above, it may prove difficult to make a case for protection as trade secrets. That is because under the Lansing definition, the disclosure of information must cause real or significant damages to the owner of the secret. In the second scenario, the fact that a multitude of persons have access to the data would also raise the question whether the owner had sought to limit dissemination by concluding confidentiality agreements.

---

2 When the Trade Secret Directive 2016/943 is transposed into German law, the legislator may well introduce a third requirement according to which the secret must have been “subject to reasonable steps to keep it secret”. German courts, by contrast, currently take the view that the owner of the information must only have intent to keep it secret, and that there is a rebuttable presumption of that intention. For details, see Anette Gärtner, “Zum Richtlinientext über den Schutz von Geschäftsgeheimnissen” [2014] N.Z.G. 650, 651; Wiebe, “Protection of industrial data” [2016] G.R.U.R. Int. 877, 880.
4 This view is shared by Flemming Moos, Marian Alexander Arnig and Jens Schefzig, “Daten als Geschäftsmodell” [2015] K. & R. Beiheft zu Heft 9, 2, 4.
8 Faccenda Chicken Ltd v Fowler [1984] I.C.R. 589 Ch D at 596: 600 per Goulding J.
9 Lansing Linde Ltd v Kerr [1991] I.W.L.R. 251 CA (Civ Div) at 259 per Stoughton L.J.
10 See section “Data as confidential information”.

Again, on a more general note the protection afforded to confidential information is limited. Depending on the circumstances of the case, third parties may be restrained from using confidential information. A duty of confidence will, however, only be imposed when a person “receives information he knows or ought to know is … to be regarded as confidential”. This limitation highlights the fact that confidential information is not considered proprietary in the sense of a right in rem. The owner of the secret must rely on a breach of confidence (actual or threatened) if he wants to bring an action.

Data as property

Can the protection provided to data nonetheless be perceived as a property-like right? The relevant criminal provisions may perhaps provide guidance.

Data-related offences under the German Criminal Code (StGB)

The StGB provides for a number of data-related offences, notably ss.202a and 303a. Section 202a prohibits data espionage, whereas s.303a StGB applies if data are deleted, rendered unusable or altered. While the prohibited acts differ, the ratio legis of both provisions is to protect the control over data.

In two fairly recent cases, the Higher Regional Courts of Dresden and Naumburg addressed the question whether breaches of ss.202a and 303a StGB sound in damages. The Dresden judges found that the defendant who had deleted emails without authorisation was not liable to damages under s.823(1) BGB, because data are intangible and thus do not enjoy protection as property. Given the breach of s.303a StGB, the claimant was, however, entitled to a cease and desist claim according to the general provisions of the German Civil Code (BGB). The Dresden Court's analysis, it was decided, related to the prohibition of acts prohibited by ss.202a and 303a StGB.

In the Naumburg case, the driver of a digger interrupted the police on whose behalf the measurements were taken, and the data contained therein were deleted. Again, the data were intangible and thus did not fall within the scope of s.823(1) BGB. The Court found that the data were confidential, i.e. a provision that is intended to protect a third party. In the Naumburg decision, by contrast, the request for an injunction under ss.1004(2), 823(2) BGB, and 202a StGB was denied. The case related to devices to measuring speed and focused on the question of who had control over data in terms of s.202a StGB. According to the court’s analysis, it was the police on whose behalf the measurements were taken, rather than the supplier of the devices, who was entitled to control.

Both decisions are silent on whether German law recognises data ownership. According to a minority view, the Dresden judgment indicates that data ownership is “conceivable”. That view perhaps entails a little wishful thinking, given that the decision is based on the understanding that s.303a StGB is a Schutzgesetz.

More importantly ss.202a, 303a StGB do not provide blanket protection to those who have control over data. If an act does not fall within the scope of the data-related offences, the affected party does not have any claims against the alleged wrongdoer. A decision of the Regional Court of Konstanz illustrates this very clearly. In the underlying case, the driver of a digger interrupted the power supply when he damaged a cable. This resulted in a massive loss of data. Nonetheless the claimant was not entitled to damages under s.823(1) BGB because data do not enjoy protection as (tangible) property. Since the requirements of none of the data-related criminal offences were met, the claimant could not rely on an alternative cause of action.

Finally, even the proponent of the minority view acknowledges that under German law the right to recovery is a necessary corollary of property. Section 985 BGB provides that the “owner may require the possessor to return the thing”. However, there is no equivalent basis for demanding access to data. The referenced decisions merely address the prohibitive rights of the person who has control over data under ss.1004(2), 823(2) BGB, 202a or 303a StGB. We can therefore conclude that German civil law currently does not recognise data as property.

The English Theft Act 1968 and common law

The High Court famously addressed data as property in the 1978 decision Oxford v Moss. Strictly speaking, the case did not relate to data but to information that was embodied in an examination paper covertly obtained by a student ahead of the exam. In contrast to the StGB and BGB, the Theft Act 1968 defines property very broadly. According to s.4(1) it also includes “intangible property”. The prosecutor therefore argued that the student had

14 Schering Chemicals Ltd v Fullman Ltd [1982] Q.B. 1 CA (Civ Div) at 14, per Lord Denning MR.
15 Campbell v MGN Ltd [2004] A.C. 457 HL at 462 per Lord Nicholls; see also Attorney General v Guardian Newspapers Ltd (No.2) [1990] 1 A.C. 109 HL at 281 per Lord Goff of Chievely.
16 A similar view is shared by Osborne Clarke LLP, “Legal study on Ownership and Access to Data” (2016), p.36.
17 Higher Regional Court of Nuremberg [2013] BeckRS 03553 (with further references); Higher Regional Court of Naumburg [2014] BeckRS 19058 at [20].
20 Higher Regional Court of Naumburg [2014] BeckRS 19058 at [20]–[30]; for more details on the debate regarding the entity that has control over data, see Peschel and Rockstroh, “Big Data in der Industrie” [2014] M.M.R. 571, 573.
stolen intangible property of the university. This did not persuade the High Court, however; it was held that, while confidential information may be protected in equity, it is not capable of being the subject of a charge of theft.28

That decision did not put an end to the discussion. In Fairstar Heavy Transport v Adkins, Edwards-Stuart J analysed authorities dating from 1893 to 2012 before tentatively coming to the conclusion that there is no proprietary right in information.29 In that case a company sought to restrain a former manager from deleting business-related emails. At first instance, the claim was dismissed on the ground that the company had no right in the emails. The judge relied on two main arguments:

1. it was unclear who should be considered the “owner” of the emails, the creator (or his principal) or the recipient(s);

2. The implications of an erga omnes right to data: “The implication … is that in principle the creator of an e-mail would be able to assert his title to its contents against all the world … It would be very strange — and far reaching — if the creator of an e-mail could require any recipient of it, however far down the chain, to delete it …. But if he cannot do this, what is the use of having this proprietary right?”30

The first argument is not entirely convincing. As mentioned above, ss.202a, 303a StGB also raise the question who shall have control over data in terms of the Act, and there is considerable debate in legal literature. However, the predominant view appears to be that data control vests in the creator, because this approach safeguards legal certainty.31

The second argument has more appeal. Fairstar Heavy Transport v Adkins indicates that, if one were to accept a concept of data ownership, it might perhaps be necessary to distinguish between different objects of protection. Tellingly, when the Court of Appeal heard the case, Mummery LJ expressed the view that it should be decided in accordance with the law of agency.32 He also urged the judiciary from discussing data ownership on a general basis:

“The claim to property in intangible information presents obvious definitional difficulties, having regard to the criteria of certainty, exclusivity, control and assignability that normally characterise property rights and distinguish them from personal rights … It would be unwise, for example, for this court to endorse the proposition that there can never be property in information … Some kinds of information, such as non-patentable know-how, are more akin to property in their specificity and exclusivity than, say, personal information about private life.”33

While this statement was obiter dictum, it confirms the view that the law is not yet settled. That is also in line with subsequent case law. In Your Response Ltd, the Court of Appeal held that a lien cannot apply to electronic data. The judges emphasised that the common law lien is a right to continue actual possession of goods and deliberately left open whether a database constitutes property.34 As regards England, the answer to the question about data ownership therefore is less clear-cut than in Germany. If a distinct right to data does exist, the courts are yet to “discover” it.

**Interjection—what would be the economic rationale for creating a right to data?**

The economic discussion is underway, but so far it seems that no one sees an urgent need for creating a right to data. One reason for granting IP rights is to incentivise the creator to innovate, leading to the generation and disclosure of more intellectual property.35 However, there is no apparent need to incentivise the collection and analysis of data.36 Data ownership arguably would not facilitate the “sale” and “licensing” of data either, because data are already the subject of transactions. Commercial parties routinely agree on data “ownership” and access rights on a contractual basis.37 Indeed, there are valid concerns that the creation of an erga omnes “monopoly” right to data might render it more difficult to access data,38 thereby frustrating and damaging further development of existing and new products and services. With all due caution, it would thus appear that there is neither a pressing need nor an obvious benefit to develop a legal framework for the digital economy that recognises a new data property right. Put bluntly: “If it ain’t broke, don’t fix it”.

---

28 Oxford v Moss (1979) 68 Cr. App. R. 183 186 per Smith J.
29 Fairstar Heavy Transport v Adkins [2012] 2 C.L.C. 795 (BDB at [30]-[58], per Edwards-Stuart J.
30 Fairstar Heavy Transport [2012] 2 C.L.C. 795 at [61]-[64] per Edwards-Stuart J.
31 Higher Regional Court of Naumburg [2014] BeckRS 19058 at [21]; B. von Heintschel-Heinegg et al. (eds), Beck’scher Online-Kommentar StGB (München: C.H. Beck, 2010), §202a, para 8 with further references.
32 Fairstar Heavy Transport v Adkins [2013] 2 C.L.C. 272 CA (Civ Div) at [46] per Mummery LJ.
33 Fairstar Heavy Transport [2013] 2 C.L.C. 272 at [47], [48] per Mummery LJ.
34 Your Response Ltd v Datateam Business Media Ltd [2015] Q.B. 41 CA (Civ Div) at [10]–[12], [17] per Moore-Bick LJ.
Pan-European data protection regulation began in earnest in 1980, and we are currently in a state of transition towards the more stringent requirements of the General Data Protection Regulation (the GDPR) which comes into force on 25 May 2018.

Neither the current nor the forthcoming data protection regimes applies to all types of digital information; rather they are relevant only to “personal data”. In order to qualify as “personal data” information must relate to a living identified or identifiable natural person. The scope of what is considered to be personal data is evolving and is broadening (for example, the Breyer case confirmed that the dynamic IP address of a computer connected to the internet, without any further information, was capable of sufficiently identifying an individual to qualify as “personal data” in some circumstances). The scope of personal data is being further extended in the GDPR by the specific inclusion of online identifiers and location data, among other things.

Individuals have well-defined rights in respect of their own personal data; for example, the right of access to their data held by a “data controller” organisation, a right to prevent personal data being used for direct marketing purposes, and a (qualified) right to require their data to be deleted. Data protection law was first introduced to protect the privacy of individuals in the face of unprecedented mass automated handling of information about them. European data protection law therefore grants people a degree of autonomy over the digital information held about them by governments and commercial enterprises, including what it is used for and how it is disseminated. However, the focus has never been to grant individuals an economic right or complete autonomy in respect of their information.

With this background, it is noteworthy that the GDPR introduces a new right for individuals which—while falling short of a property right, as such—could be seen as a step towards treating data as a commodity. The so-called right to data portability[46] entitles an individual to be provided with a machine-readable copy of the data which they have provided to a “controller” organisation or to require that organisation to transmit the data to another organisation nominated by the individual.

What information does the portability right apply to? First, it has to relate to the individual, so that excludes anonymous information or data that do not relate to the individual. Secondly, the data must also have been provided by the individual. This has been broadly interpreted in the Article 29 Working Party’s guidance on the data portability right (Guidance),[46] namely as including (1) information provided directly by the individual, such as name and address, and (2) observed data about the individual, provided by virtue of the use of a device or service, e.g. search history, traffic data and location data or even other raw data such as the heartbeat tracked by fitness or health trackers. This is highly significant for big data applications. It appears to open up the field of telemetry and remote sensor data to compliance with the data portability right, which could involve the enforced transmission from one industry participant to a competitor of very extensive data collections indeed. It should be noted that, at the time of going to press, the European Commission has indicated that, by extending to observed data, the Guidance goes beyond what it was agreed the portability right should cover.[47]

The Guidance indicates that the data portability right should not lead to the compromising of proprietary intellectual property of the data controller. It should not extend to data that are exclusively generated by the data controller (so-called inferred data or derived data), such as a user profile or individual credit score or analysis resulting from the application of an algorithm. A personalisation or recommendation created by the controller company would also be excluded from the pool of data potentially subject to the data portability right.

Life will not be entirely simple for the receiving “new” data controller, however; the ported personal data come with the customary data protection restrictions attached to them. Processing purposes must be compatible with the purpose of the transfer. Otherwise, such processing is likely to be unlawful and unfair, especially if any third parties’ data are also included in the “ported” data and they are not informed and cannot exercise their rights as data subjects. Controller organisations likely to hold data which lends itself to portability are encouraged now to

---

46 Regulation 2016/679, which comes into force on 25 May 2018.
47 In some EU Member States, the Data Protection Directive 95/46 has been implemented to include data relating to legal persons, not just natural ones: for example, Austria and Greece.
48 Breyer v Bundesrepublik Deutschland (C-582/14) EU:C:2016:779; [2017] 2 C.M.L.R. 3.
49 GDPR art.4(1) “Personal data” means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person” (newly listed concepts emphasised).
50 A “controller” or “data controller” is an organisation or other legal person which decides the purposes for which, and the manner in which, personal data are processed (the “how” and “why” behind the use of the personal data); a controller is subject to the full obligations imposed by data protection law. See GDPR art.4(7) for the definition applicable from 25 May 2018. “Data controller” and “controller” are used in this article interchangeably.
51 GDPR art. 20 states that an individual “shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided”, where the processing is based on consent of the individual or is necessary for the purpose of a contract with the data subject.
52 The Article 29 Working Party was established under the Data Protection Directive (95/46) and is an independent European advisory body to the European Commission on data protection and privacy.
54 The head of Justice Commissioner Vera Jourová’s cabinet, Ms Renate Nikolay, reportedly spoke about the Commission’s scope concerns at a Humboldt University Law Clinic in Berlin on 20 April 2017.
build systems and adopt application programming interfaces which are compatible with the forthcoming enhanced right to data. The most obvious sectors are utilities and telecommunication service providers and banks, but in principle the portability right is sector-neutral. How it may impact on connected and autonomous and semi-autonomous vehicle manufacturers remains to be seen.

According to the Article 29 Working Party, the data portability right in the GDPR is expected to foster the development of new services in the context of the digital single market strategy. While the GDPR is individual-focused legislation rooted in protecting fundamental human rights, it empowers individuals with the ability to move a portfolio of their data from one commercial enterprise to another (probably competing) enterprise. The exercise of that right could have considerable economic value for the receiving enterprise, not least because of the expanding scope of “personal data” which is tending to bring within its remit information which previously was considered merely technical, automatically recorded data. Presumably we will see this economic value reflected in the incentives offered to individuals who bring “their” data with them in future.

Conclusion and outlook

Neither German nor English law currently recognises a discrete “data ownership” right. From an economic perspective, there are valid concerns that the introduction of a new monopoly right might frustrate the development of existing and new products. The idea of creating a right to data does not sit easily with the GDPR or, more specifically, the data portability right. The case for a new data property right therefore appears as yet unproven. However, the outcome of the European Commission’s current consultation is pending at the time of writing and therefore it is feasible that a decision may yet be taken to lay the foundations for such a right. The project certainly enjoys strong support from some quarters.  