

FEDERAL LAWYER

The Magazine of the Federal Bar Association

The Implications of COVID-19 for Incarcerated Individuals Seeking Legal Redress

page 36



Intersection of Intellectual Property and Privacy Rights

By Renata Lowenbraun and Hannah Shaw



Renata Lowenbraun is vice president of Legal at Prove, a leading provider of mobile authentication and ID solutions, where she is responsible for strategic technology transactions, intellectual property, privacy, and litigation. Hannah Shaw is a third-year law student at New York Law School and a legal intern at Prove, where she specializes in intellectual property. ©2021 Renata Lowenbraun and Hannah Shaw. All rights reserved.

The views and opinions expressed in this column are those of the authors and do not necessarily reflect the views or positions of any entities they represent.

While the changing legal landscape concerning the privacy rights of individuals has been a primary focus for most companies lately, we should also be paying attention to its impact on intellectual property and proprietary rights of companies. Legal ramifications concerning advancements in data procurement and organization, and current and future regulations of personally identifiable information (PII), are sometimes ambiguous and challenging to interpret.

Regulation of Personally Identifiable Information United States

Currently in the United States, a plethora of separate laws regulate the treatment and security of PII, including the Federal Trade Commission Act, the Gramm-Leach-Bliley Act, the Health Insurance Portability and Accountability Act (HIPAA), the Telephone Consumer Protection Act, the Fair Credit Reporting Act, and others that are beyond the scope of this column.¹ Instead of having one controlling piece of legislation, the United States has these laws, with each regulating particular industries or uses of PII.

De-identification, pseudonymization, anonymization, and re-identification (along with other terms of art) are useful tools for companies to protect PII while also complying with the various rules and regulations. Generally speaking, although definitions vary by applicable law or regulation, “de-identification” is generally defined as “removing the association between a set of identifying data and the data subject.”² Anonymization, on the other hand, refers to “remov[ing] the association between the identifying data set and the data subject.”³ Finally, pseudonymization means “remov[ing] the association with a data subject and add[ing] an association between a particular set of characteristics relating to the data subject and one or more pseudonyms.”⁴ Several regulations and acts of Congress have included statements that establish that if PII has gone through one of the above steps, the

same level of compliance is not necessarily required. One example is a section within HIPAA that clarifies that when a piece of PII [or, as HIPAA refers to it, protected health information (PHI)] has been de-identified, it is no longer considered protected and therefore not afforded the same regulation and restrictions.⁵ However, if PII is re-identified using a key, the PII that has been re-identified is once again considered protected PII.

Though Congress has taken no specific actions as of yet, several states have decided to enact their own stringent protections. One of these states is California, which passed the California Consumer Privacy Act (CCPA) in 2018. The CCPA allows for any California consumer to request to see all the information a company retains about them.⁶ Additionally, Virginia passed the Consumer Data Protection Act (CDPA) in March 2021. The CDPA has essentially the same effects as the CCPA except for the fact that employee data is not included in the data that may be requested from a company.⁷ Additionally, several states, including New York and Texas, are in the process of passing their own versions of the CCPA and CDPA.⁸

European Union

Within the European Union (EU) there exists a more centralized regulation of PII under the General Data Protection Regulation (GDPR).⁹ The GDPR is often considered the strictest form of regulation of PII currently in existence that is not sector specific. However, unlike HIPAA in the United States that provides for specific methods for de-identification, the GDPR defines only the concept of “anonymization” and “pseudonymization.” Where data is anonymized, the data is no longer subject to GDPR because personal identifiers have been removed and cannot be re-identified. When data is pseudonymized, such as where a company uses coded data that is no longer attributed to a specific data subject but links it to additional information kept separately, such data continues to be subject to the GDPR.¹⁰ Since the creation of GDPR, various regulatory bodies charged with interpreting or regulating it have rendered opinions and decisions as well.

Copyright Protections and Sui Generis Protection for Data Copyrightability of Databases and Sui Generis Protection for Databases

United States

Once a company has de-identified or pseudonymized the PII that was received and organized it into a usable database, legal interpretation concerning intellectual property or rights of companies in light of emerging privacy laws makes such analysis more challenging. Generally, data, which includes de-identified PII, is not copyright protectable. However, a database may be copyright protectable due to it being considered a “compilation,” which is one of the categories in the Copyright Act of 1976.¹¹ The Copyright Act of 1976 (the “Act”) defined “compilation” as “a work formed by the collection and assembling of preexisting materials or of data that are selected, coordinated, or arranged in such a way that the resulting work as a whole constitutes an original work of authorship.”¹² Though it would appear that databases are entirely protected under the Act, there are some court-created requirements that have been established to meet the originality requirement pursuant to the act.

In *Feist Publications v. Rural Telephone Service Co.*,¹³ the Supreme Court held that in order for a compilation to be protectable, there has to be some element of creative originality. *Feist* involved a dispute between two separate publishers of telephone books. Rural Telephone Service Co. (“Rural”) was a local telephone company that published a telephone directory that covered its service area. Feist Publications (“Feist”) was a publisher of telephone directories that covered several service areas. Feist sought a license to the listings included in Rural’s directory, and when they were refused, they decided to copy Rural’s listings and add them to their own directory, nonetheless. Rural brought suit against Feist for copyright infringement of its listings.

The court, in its holding, refined the Copyright Act of 1976’s definition of compilation. The court clarified that Congress still specifically required originality with regard to the organization of the compilation instead of simply having copyright protection for any form of compilation. The elements of authorship creativity that are required were outlined by the court as the selection, coordination, and arrangement of the underlying material.¹⁴ In *Feist*, the court found that there was no element of originality in the way that Rural was listing the directory and that therefore, it was not copyrightable. Due to the lack of copyrightability, Feist’s copying of the database (directory) was not found to be infringement. Additionally, in *Feist*, the court found importantly that the underlying data that would be within the compilation is not copyrightable and that only the organization of the data is.

Additionally, in the United States, no sui generis protection for databases currently exists. Sui generis protection means the protection of the creation of the database versus the arrangement and organization of the database. There were several attempts by members of Congress to establish this protection; however, it was never passed.¹⁵ The general concern with this type of protection was that it would stifle innovation and go against the U.S. Constitution’s design of promoting progress in the arts and sciences.

European Union

In the EU, a Database Directive provides two separate rights for protection of a database,¹⁶ with one—a copyright protection for the organization and structure of the database itself—being similar

to that of the United States. Additional to copyright protection, however, the directive contains a separate sui generis protection for the database.

The concept behind sui generis protection is that, as a reward for an individual’s or company’s “substantial investment,” the database that was created is afforded protection against acts of extraction or reutilization. This “substantial investment” is meant to provide for the safeguard of the data itself due to the lengths that the creator of the database went through to collect the data.¹⁷ The protection against extraction or reutilization prevents individuals or companies from taking large parts of the database without the express consent of the originator of the database. As mentioned above, it prevents the reutilization, which means making the information in the database available to the public. Importantly, there is a very large exception to these rights: that “insubstantial parts” are excluded from protection. This section of the Database Directive means that the maker of the database cannot prevent a lawful user of the database from extracting or reutilizing insubstantial parts of the database for any reason. Additionally, the term for which the sui generis protection lasts is only 15 years as opposed to the term provided for copyright protection, which is, as a general rule, 70 years from the time of an author’s death.¹⁸

Additionally, there are some developing concerns over the rights of data subjects under GDPR and whether they are entitled to the portability of their data contained in database tables of companies when such companies own sui generis or copyright interests in the database tables. Currently, there is no definitive answer from the regulatory bodies of the GDPR member states. However, in the coming years, an answer is very likely.¹⁹

Derivative Works and Data

Generally, the owner of the original copyright has an exclusive right to “derivative works.” Derivative works means those that are based upon the original work. Examples of derivative works include movies based on books and new musical arrangements of an original composition. While database tables, and generally not the underlying data itself, are protectable as copyright, in *Feist*, the court also held that the protection for the organization of the data itself could be protectable as organized in the database table, but that such protection was “thin.”²⁰ At first, the meaning of “thin” was unclear to courts applying *Feist*; however, lower courts have interpreted it to mean that only the specific arrangement of data in the database is protected, and it would be very difficult to enforce the copyright against derivative uses of the data by third parties when the same underlying data has been reorganized in a new and original way.

In interpreting *Feist*, subsequent lower court decisions have made clear that, although there is protection for the original database table, they have generally not found infringement to occur when data from the table is directly copied by third parties due to the thin nature of the copyright protection. These cases seem to suggest that generating a reorganized database table may be afforded its own intellectual property protection as an original work.

For example, in a second circuit case, *Key Publications, Inc. v. Chinatown Today Publishing Enterprises*,²¹ derivative rights to the data in a yellow pages address book that Key Publications, Inc. (“Key”) published was not enforceable against Chinatown Today Publishing Enterprises (“Chinatown Today”) when Chinatown Today directly copied the data (the listings) into a new original database table. In

essence, the court determined that the data copied was not organized in the same manner as Key published it, and thus, there was no infringement. Additionally, it found that not only did Chinatown Today not infringe but that its organization of the data into its own original work entitled it to its own copyright protection.

Fair Use Doctrine

There is also case law that suggests that data in database tables may constitute fair use under the doctrine set forth in 17 U.S.C. § 107. In other words, if a copyrighted work is being used in a particular way—such as for criticism, commentary, teaching, research, and news reporting—it may qualify as fair use and would not be infringing upon the copyright. Such factors in determining fair use are the following: the purpose and character of the use, the nature of the copyrighted work, the amount and substantiality of the portion used, and the effect of the use on the potential market.

In *Campbell v. Acuff-Rose Music, Inc.*,²² a music group decided to make a parody of a copyrighted song without receiving permission from the owner of the copyright. The court held that parodies were covered under Section 107, but most importantly, the court held that not all the factors are weighted equally in determining fair use. They found that if the first factor weighed more in favor of fair use, then the other factors were less important.

More recently, in *Google LLC v. Oracle America Inc.*,²³ the court further expanded the fair use doctrine in the context of software and information. In *Google*, Google was writing a code to be used for its Android phones, and while writing this code, it was using calling functions that were Javascript, the copyright of which is owned by Oracle. Google used 11,500 lines of code to write a whole new program. The court ended up holding that Google's use of Oracle's code was fair use and therefore not copyright infringement.

While this particular case was not specifically about database tables, the future will see whether this holding will expand into the subject area considered in this column. The court put a heavy emphasis on the fact that Google's use of the code was to create a whole new program that would help many more individuals. In his opinion, Justice Breyer wrote that the fair use doctrine "permits courts to avoid rigid application of the copyright statute when, on occasion, it would stifle the very creativity which that law is designed to foster."²⁴ In this excerpt, Justice Breyer makes clear that when a large amount of creativity and innovation is at stake, the copyright rules can be bent.

As data and information received and used by companies are becoming more valuable with new and emerging technologies, we should expect more caselaw expounding on privacy and intellectual property rights and how they interact. With the increasing willingness of countries to regulate PII and other forms of personal information, the landscape will likely change rapidly, and it is worth keeping up to date. Moreover, the expansion of regulations of PII may have a vast effect on the underlying intellectual property and proprietary rights in PII. ©

Endnotes

¹*Data Privacy Principles all Legal Providers Should Adopt*, THOMSON REUTERS, <https://legal.thomsonreuters.com/en/insights/articles/data-privacy-principles#:~:text=In> (last visited Dec. 28, 2021).

²INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, HEALTH INFORMATICS – PSEUDONYMIZATION (ISO/TS 25237) (Dec. 2008), <https://www.iso.org/obp/ui/#iso:std:iso:ts:25237:ed-1:v1:en>.

³*Id.*

⁴*Id.*

⁵Simon L. Garfinkel, *De-Identification of Personal Information*, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, NISTIR 8053 (Oct. 2015), <http://dx.doi.org/10.6028/NIST.IR.8053>.

⁶CAL. CIV. CODE §§ 1798.100-1798.199.

⁷VA. CODE ANN. §§ 59.1-571-59.1-581 (2021).

⁸Sarah Rippey, *US State Privacy Legislation Tracker*, INTERNATIONAL ASSOCIATION OF PRIVACY PROFESSIONALS (June 8, 2021), <https://iapp.org/resources/article/us-state-privacy-legislation-tracker/>.

⁹James Alford, *GDPR and Artificial Intelligence*, THE REGULATORY REVIEW (May 9, 2020), <https://www.theregview.org/2020/05/09/saturday-seminar-gdpr-artificial-intelligence/>.

¹⁰JOHNS HOPKINS MEDICINE, PREPARING FOR THE EU GDPR IN RESEARCH SETTINGS (May 22, 2018), https://www.jhsph.edu/offices-and-services/institutional-review-board/_pdfs-and-docs/GDPR_Application%20in%20Research%20Settings.pdf.

¹¹17 U.S.C. §§ 101-122.

¹²*Id.* at § 103.

¹³*Feist Publ'ns, Inc. v. Rural Tel. Serv. Co.*, 499 U.S. 340 (1991).

¹⁴U.S. COPYRIGHT OFFICE, REPORT ON LEGAL PROTECTION FOR DATABASES (Aug. 1997), <https://www.copyright.gov/reports/db4.pdf>.

¹⁵Mark Davison, *Database Protection: Lessons from Europe, Congress, and WIPO*, 57 CASE W. RES. L. REV. 829, 844-850 (2016) (discussing the effects of the database directive on international database law).

¹⁶Council Directive 96/9, art. 7, 1996 O.J. (L 77) 25, 26 (EC).

¹⁷REPORT ON LEGAL PROTECTION, *supra* note 14.

¹⁸*Copyright*, YOUR EUROPE (May 19, 2021), https://europa.eu/youreurope/business/running-business/intellectual-property/copyright/index_en.htm.

¹⁹Stephanie Elfering, *Personal Data Meets Sui Generis Database Right*, in UNLOCKING THE RIGHT TO DATA PORTABILITY 33-51 (2019).

²⁰*Feist Publ'ns, Inc. v. Rural Tel. Serv. Co.*, 499 U.S. 340, 349 (1991).

²¹*Key Publ'ns, Inc. v. Chinatown Today Publ'g Enters.*, 945 F.2d 509 (2d Cir. 1991).

²²*Campbell v. Acuff-Rose Music, Inc.*, 510 U.S. 569 (1994).

²³*Google LLC v. Oracle America, Inc.*, 141 S.Ct. 1183, 209 L.Ed.2d 311 (2021).

²⁴*Id.*

Editorial Policy

The Federal Lawyer is the magazine of the Federal Bar Association. It serves the needs of the association and its members, as well as those of the legal profession as a whole and the public.

The Federal Lawyer is edited by members of its Editorial Board, who are all members of the Federal Bar Association. Editorial and publication decisions are based on the board's judgment.

The views expressed in The Federal Lawyer are those of the authors and do not necessarily reflect the views of the association or of the Editorial Board. Articles and letters to the editor in response are welcome.