Will Privacy Kill the Digital Star? Analyzing Data Protection Regulations

Authors: William Hochberg & Timothy Toohey

>> Introduction

In recent years, data has produced radical changes in the music industry for performers, record labels, festivals, sponsors, managers and producers. Musicians and managers want fan data to sell more tickets, determine which cities to include on their tours, choose songs to promote in different regions, and generally to find out what is working for them and what isn't. Record labels want to know in what corners of the world their artists are connecting with fans, so they can institute better digital promotional campaigns and build on regional successes to expand into neighboring territories. They also use data to consider the potential of new acts or an artist to appeal to key demographics. Music publishers may employ data about populations and popularity of songs in particular territories to better pitch synchs for ads and programming in those regions. The data generated by streaming services, like Spotify, are also used by many sectors of the industry to provide analytics for music acts and labels to analyze fans for particular songs and acts.

But with the expanded collection of data in the music industry has come concern that our personal data may be used for improper purposes and, with that, a raft of new privacy and data protection laws and proposed legislation aimed at promoting more transparency. Laws such as the EU's General Data Protection Regulation ("GDPR"), which came into effect on May 25, 2018, require companies, including those in the music industry, not only

"The data generated by streaming services, like Spotify, are also used by many sectors of the industry to provide analytics for music acts and labels to analyze fans for particular songs and acts."

to communicate to the public what they are doing in regard to personal data, but also to have a legitimate basis for their collection and sharing of personal data. Although the United States has typically taken a less proscriptive approach, there has been a call for a GDPR-like law there as well, particularly in response to controversies such as the Facebook and Cambridge Analytica vdata scandal.[1]

Echoing the GDPR, California has passed the California Consumer Privacy Act ("CCPA"), which will come into effect on January 1, 2020, giving California residents GDPR-like rights.[2] But does the transparency of GDPR and other privacy laws threaten the productive uses to which data is placed in the music industry? Will artists, managers, record labels, festivals and others be forced to curtail their practices?

"The new laws do complicate today's entertainment and advertising businesses," says Matthew Abdo, lead digital data strategist at theAmplify, a full-service influencer marketing technology platform, part of the You & Mr Jones group. "Now if you are working with large brands that enlist influencers who have audiences in the EU, the GDPR standards are going to be applied to 'processors' and 'controllers' worldwide even for data not generated in the EU. We hold all campaigns for our clients to the same standards."[3]

While GDPR-like laws are unlikely to put Google or Facebook out of business, music professionals using social media must modify some of their practices and may have to turn to inventive ways to comply with privacy laws.

>> Understanding the Basics of GDPR and Privacy Laws

Data privacy laws have been around for several decades as technology has made it easier to collect and share information about individuals that was previously difficult or impossible to gather. In recent years, focus has turned in particular to social media platforms, such as Facebook and Google, and the potential exploitation and misuse of the personal information such platforms collect. In Europe, where individual privacy

is a fundamental right and there are considerable suspicions regarding the practices of Internet and technology companies based in the United States, privacy laws seek to redress what is seen as a power imbalance between collectors and processors of data, on the one hand, and "data subjects," as they are called in GDPR parlance, on the other.

Following are some details concerning these laws and how they relate to music and media businesses.

1) The ABC's of GDPR

GDPR applies to all 27 member states of the EU (including the United Kingdom pre-Brexit) and companies worldwide collecting data from EU residents, and is undoubtedly the most significant privacy legislation passed by any jurisdiction in the world.[4]

The GDPR regulates the collection and processing of "personal data" of EU residents by a "controller" of data. "Personal data" is broadly defined as "any information relating to an identified or identifiable natural person ('data subject')."[5] A "controller" is a natural and legal person who "alone or jointly with others, determines the purposes and means of the processing of personal data."[6] "Processing" is broadly defined as "any operation or set of operations which is performed on personal data or on sets of personal data..."[7]

Key to the GDPR is the requirement that the collection and processing of the personal data of EU residents—whether by companies located in the EU or those outside of the EU—requires a legal basis. The most common legitimate bases for processing include (i) processing of information that is necessary for performance of a contract to which the data subject is a party (e.g., fulfillment of an order from an e-commerce site); (ii) processing necessary for compliance with a legal obligation to which the controller is subject; (iii) processing necessary for the purposes of the legitimate interest pursued by the controller or by a third party, except where overridden by the interests or fundamental rights of the data subject; and (iv) consent by the data subject for processing of his or her personal data "for one or more specific purposes."[8] The latter basis for collection is typically called

"opt-in" consent, e.g., when a data subject ticks a box to receive information about future performances of a particular band or about a certain festival.[9]

Notably, processing by opt-in consent must be "freely given."[10] The GDPR requires transparency in the process. Not only must the individual whose consent is requested be apprised of what information is being collected and the purposes of the collection, but the request must be presented using "clear and plain language."[11] Data subjects under the GDPR are also given significant rights to obtain information about the data collected by them, but also rights to opt-out of future collection of information. The GDPR imposes further restrictions on collection of information from children and "special categories" of data related to racial or ethnic origin, political opinion, religious beliefs, genetic and biometric data, or other personal data.[12]

2) US Sectoral Laws Come Into the Picture

In contrast to the GDPR approach, data privacy laws in the United States are a patchwork of federal and state law that deal with a much more limited scope of "personal information" (sometimes called "personally identified information" or "PII").[13] There is no comprehensive federal privacy law, but rather laws relating to categories such as protected health information (HIPAA),[14] financial information (the Gramm-Leach-Bliley Act)[15] and data for persons under the age of 13 (COPPA).[16] Under the federal system of the US, additional state laws relate to protection and reporting data breaches of a restricted category of personal information, including Social Security Numbers, credit card numbers, drivers' licenses, and login information and passwords. As noted, the trend in the US may be turning to more proscriptive and comprehensive laws, as evidenced by the CCPA, which will govern a broad reach of personal data defined in terms similar to the GDPR such as "information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household."[17] Notably, the passage of the CCPA has led to calls at the federal level for a comprehensive privacy law that would preempt inconsistent state laws.[18]

3) Business Approaches to Transparency-Focused The data Generated

by Streaming Services, Like Spotify, are Also Used by Many Sectors of the Industry to Provide Analytics for Music Acts and Labels to Analyze Fans for Particular Songs and Acts. Privacy Laws

Both the GDPR and privacy laws under consideration in other corners of the globe enshrine transparency and consumer disclosure and, in some instances, control, as key elements.[19] Transparency requirements are meant to combat information fatigue that occurs when an end user clicks without reading frequently convoluted technical communications, including privacy policy disclosures. European authorities have criticized statements such as "We may use your personal data to develop new services" as being insufficiently detailed, because it is unclear what the new services are or how the data will help to develop them. [20] Similarly, US privacy laws have adopted privacy disclosures, albeit in the form of lengthy privacy policies that are anything but easy for a consumer to read.[21]

Whereas before GDPR, music festivals would ask a fan purchasing tickets online months before the festival if they wanted to check a box to obtain notifications about changes to the bill and other important updates that a fan may want to know about, while "whispering" in small print that information may be shared with sponsors, post-GDPR practices among many festivals, even ones outside of the EU, are careful to obtain permission to use or share any data with a particular named sponsor.

Some festival executives have noticed that fans don't seem to mind giving permissions more often since GDPR practices have been adopted and are still willing to engage with sponsors whom they know, or should know, will use their data in commerce, all in exchange for closer ties to their favorite artists. But sponsors are still wary. Where a sponsor may have paid $500,000 to have its name on a main stage at a major festival in the past, or several million for a slate of festival stages, many are said to be more guarded about committing major funding where valuable data may be less available than before.

"Transparency requirements are meant to combat information fatigue that occurs when an end user clicks without reading frequently convoluted technical communications, including privacy policy disclosures."

4) Scrub and Scrape is the New Rock and Roll in Personal Data

The GDPR acknowledges the legitimacy and utility of data collection practices that do not expose individually identifiable data and has embraced the "pseudonymization" of data, which it defines as "the processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information."[22]

Similarly, United States privacy law has embraced the use and sharing of data that strips out individual identifiers. For example, the CCPA will provide California consumers with the right to opt out of such sharing however again with the proviso that "deidentified" or "aggregated" consumer data may continue to be shared with third parties.

As discussed below, in reference to the music industry, the bottom line trend is that "pseudonymized," "de-identified," or "aggregated" data (even if it originates from what would otherwise be defined as "personal data" or "personal information") may be used and shared for purposes that would otherwise not be permissible.[23]

>> Back to the Future: Does the Music Industry Need All This Data to Succeed?

Restrictions of GDPR and other privacy laws may bring music marketing back to an earlier time, some say. It is sometimes forgotten how significant an effect digitalization and data collection have had on the music industry. In the 90's, before the music industry was fixated on data mining, targeted advertising, and streaming playlists, a big hair band might have gained a foothold in a foreign territory by simply putting their platform boots on the ground.

For instance, in the early 90's, Los Angeles-based hard rock band Mr. Big focused on Japan the old-fashioned way by getting to know the culture and meeting and greeting fans and key music industry players during extended annual tours not only between Tokyo and Osaka, but also into the Japanese hinterland. This approach paid off by the mid-2000s, as the band reportedly became the second most popular foreign act in Japan,

after Bon Jovi.[24] To this day, Mr. Big, mainly remembered in the U.S., if at all, for one hit called To Be With You, remain "Big in Japan". In earlier decades, Buddy Holly and the Crickets initially broke bigger in England than in America initially, and John Lennon and the Beatles[25] broke out of England to take over the world thanks to America's fabled disc jockeys Murray the K and Alan Freed.[26] Would these bands' treks to success have been different or quicker with e-commerce, fan relationship management, and private data about dedicated followers and their lookalike populations?

Today, playlist placements on platforms like Spotify can break an artist with lightning speed, remarks Piero Giramonti, a music executive and former head of Capitol Records' Caroline division and Harvest Records. One of his signings, the artist Banks, had skyrocketing success after a music video for her song "Waiting Game" was placed in a Victoria's Secret commercial shortly after its release in 2013. "She had a little bit of recognition on SoundCloud and elsewhere up to that point," Giramonti recalls. "But after Victoria's Secret placed the song in a TV commercial, the thing blew up on Spotify and then three of the other tracks on her EP also blew up. Within a few weeks, we went from streaming 10,000 plays per track per week to streaming 10 million plays per track per week."[27] This kind of exposure led to her songs getting put on more playlists, which in turn led to a streaming explosion.

Playlists, ad syncs, and data analytics have become today's way to rise above the din of competition. Targeted ads to fans and social media-infused sales pitches to potential sponsors are a function of a music industry far more complex and siloed than in the late 50's and early 60s'. The emerging data practices in various aspects of the music industry have produced changes through the related forces of digital distribution and data generation in the fields of touring and festivals, recording and production, and in fan-based marketing and sponsorship.

How might various sectors of the music industry handle the challenges of the GDPR era? Here's a breakdown.

"The emerging data practices in various aspects of the music industry have produced changes through the related forces of digital distribution and data generation..."

1) Fests Keep on Festing

Festivals generally use fan data in three ways. First, festivals attempt to attempt to entice and sign sponsors by giving them access to music fans' personal data, including age, gender, household income, location, and email addresses. Essentially, the festivals are "selling" the data to the sponsor, even if the transaction does not look like a sale. Let's say a fast food chain wants to reach a festival crowd. It may be more willing to pay millions in sponsorship funds if in addition to placement of its logo on a slate of festival stages and in online marketing, the restaurant chain can also obtain data about where festival goers are dining and what kind of food they're eating before and after the festival, so they can gauge the success of the campaign and learn how to better reach the fests' key demographic and drive them to their restaurants.

The second common data practice is that festivals use data internally to learn how to sell more tickets and to create target audiences for ad campaigns. Under this practice, the festivals will use the data that they collect not for specific marketing activities towards a specific individual, but for more general analytical purposes.

Finally, festivals use data for operational purposes such as finding out how many fans per minute are entering a park so they can improve the layout, lessen congestion, and improve safety. Again, the purpose is not targeting of specific individuals, but analyzing consumers more generally.

Of these three practices, the GDPR and other privacy laws will have the biggest impact on the outside marketing and sponsorship piece, because it may potentially involve sharing of personal data with a third party, i.e., the sponsor or marketing partner.

Although a festival attendee may opt-in to collection of personal information by the festival itself, under the GDPR that consent would not extend to collection of data by unspecified sponsors. Nor would the festival's interest in making money through such sponsorships constitute a "legitimate interest" for sharing the information with third parties.[28]

Festivals might possibly to come up with a "just in time" opt-in notification for tie-in or sponsorship offers at the festival itself, but a generalized statement in a privacy policy would neither be sufficiently transparent, nor constitute a legitimate basis for sharing the personal data of attendees under the GDPR.

Festivals in the United States would generally not be subject to such restrictions at least to the extent that they do not involve collection of data from EU residents. However, if the CCPA comes into effect they may have to grant consumers in California an "opt-out" right by installing a "Do Not Sell My Personal Information" link prominently on the home page of their website.[29] This requirement would potentially be difficult for festivals to implement because it may not be possible to calibrate sharing of personal information on a customer by customer basis. Rather than doing so, a festival may instead decide to not share information with any third parties.

Aside from legal requirements, festivals who share personal data with third parties must keep in mind the trust festival attendees have in the festival brand. The festival world is booming at the moment with events such as Coachella and Lollapalooza becoming cultural phenomena. An estimated 32 million fans attend at least one music festival in the US alone every year,[30] almost all of them wearing RFID wrist bands tracking their movement and purchases, while tens of millions of fans download festival apps that take their email addresses and other key data in exchange for directing them to the right stages and helping them feel closer to their favorite bands. Given their popularity, it may appear that many fans are quite oblivious to their data.

But the growth of sponsorship and the unrestricted mining of personal data might sour the vibe of the trusting relationship between fans and not only their favorite bands, but also with their favorite festivals. The trust between the music devotee and the festival is what the sponsors are buying. It is hard to assess at this early stage whether the transparency that is demanded by the GDPR and other privacy laws will chill or kill the fan-to-fest relationship, or whether the festival business will continue to expand year after year unabated.

2) Transparency in the Recording and Publishing Businesses

Since the Napster-fueled crash of the recorded (and published) music industry in 2001 to the optimistic outlook of today's record business rebound, conference keynote speeches have transitioned from "End of Days" scenarios to "Days of Wine and Roses" promises. To understand why GDPR threatens to kill the buzz, one must consider how old school music business practices have adapted lately.

Traditionally, music publishing has been viewed as a passive "penny collecting" business where the publisher's first job is to collect income from licensees and performing rights organizations, and their second job is to pay their songwriters on time. "The more active publishers are heavily focused on pitching songs for various types of placements, and this is where data analytics can affect their business and creative decisions" says Miles Feinberg, founder of Music Rights Group, and former EVP of Music Sales Corp. "Publishers' sync teams are pitching songs for film, television and advertising for the most part," he says, "and they can use analytics based on age range, locations, and various other factors to determine what compositions might trend well for a use specifically targeting a certain demographic or region where the figures suggest that a certain song or genre would fit well."[31]

Generally, publishers are less involved in demographic targeting than record companies. Songwriters are invisible compared to artists who engage with fans and are often marketed like products for public consumption. Accordingly, publishers are not the ones collecting personal data from music fans themselves, and are not typically involved in the problem of getting permission from fans. If they need to obtain permission, it will come from licensors.

Most often, publishers seek to obtain analytics gleaned from data obtained by streaming portals, record labels, and social media platforms, to the extent those parties are permitted to share that data.

But just as record companies nowadays base many of their signing and marketing decisions almost solely on the demographics and engagement statistics of the followers of young artists, so do music publishers, who follow the lead of labels when it comes to how data impacts their business. Publishers aren't targeting populations to sell a product as much as appealing to ad agencies and producers of film and TV to pitch songs that will, theoretically, appeal to those targeted populations. For example, a publishing sync team may target U.S. females age 13-16, EU urban males age 16-30, or UK classic rock fans over 40, relying on an artist's Twitter, Facebook, Instagram followers, and if the demographic matches up, then the publisher or label may decide to throw more resources at pursuing that target.

As with the data collections by festivals, the use of aggregate or pseudonymized data from streaming services by producers, publishers or bands, would likely not be subject to the GDPR because it would not involve individually linked and identifiable data. The collection of general demographic data regarding the appeal of a particular act on social media or similar information from a streaming service, such as Spotify, Apple Music or SoundCloud, even if used for marketing purposes, does not run afoul of the data collection and processing regulations of the GDPR.

The use of artists' e-mail lists is another matter, however, when it comes to both GDPR and CCPA compliance. Under the GDPR, an artist would likely have a legitimate interest in keeping up with his or her fans, just as any brand would have a right to inform its followers of new product offerings. Under most circumstances, the opt-in consent from a fan—if the purposes were properly disclosed by the artist to the fan—would be sufficient as long as the fan was allowed to opt-out of future communications and (more importantly) uses of his or her data by the band. The transparency and rights afforded to data subjects under the GDPR require such compliance.

The sharing (or sale) of this information by a band to a third party, such as sponsor, would most likely not be permissible under the GDPR because most existing privacy policies only describe third parties generically (e.g., "marketing partners") and not by

name. This would particularly be the case for consent that was obtained prior to May 25, 2018, when the GDPR came into effect, which would not be either explicit or ambiguous.

>> Conclusion

Transparency laws will not kill the digital star, but they may slow her down, as all facets of music and media companies have become increasingly dependent on new and improved data mining techniques. However, human touch, inspired hunches, and face-to-face contact that have launched and sustained superstar careers in the past, may gain ascendancy over the analytics worship so prevalent in today's music and media industries.

In the old days, a major label made decisions based on 25% marketing data and 75% human interaction the artist and others. More recently, that ratio has reversed but the pendulum may be swinging back, says music executive Piero Giramonti. "In every A&R meeting, you look at the numbers, how much does it stream, where are the streams coming from," Giramonti says. "But you don't blindly allow that data to dictate the decisions and investments of hundreds of thousands of dollars on signing an artist and making and marketing a record. You need to meet the artist. Do they have ambition? Do they have the intellect to handle the trials and tribulations of making a career out of being an artist? The data doesn't tell the whole story by any means."[32] Even if GDPR and its offspring curtails the marketplace for analytics and algorithms, the rhythms and rhymes that have captivated audiences since cave-dwelling days will keep on coming.

[1] *The Cambridge Analytica/Facebook scandal in early 2018 involved the surreptitious collection of personal data of over 87 million Facebook users by a firm associated with political causes, including Brexit and the candidacy of Donald Trump, that used the data to attempt to target voters. See M. Rosenberg, N. Confessore and C. Cadwalladr, How Trump Consultants Exploited the Facebook Data of Millions, New York Times, March 17, 2018, available at https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html*

[2] *The CCPA will be codified at Cal. Civ. Code §§ 1798.100-1798.199. The official text of the CCPA as passed may be found at https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375&search_keywords=Consumer+Privacy+Act+of+2018. As of the time of the writing of this article, there were several proposals to amend the text of the CCPA.*

[3] *Authors' interview with Matthew Abdo.*

[4] *The full text of the GDPR may be found at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN*

[5] *GDPR Article 4(1).*

[6] *Id. Article 4(7).*

[7] *Id. Article 4(2).*

[8] *Id. Article 6(1).*

[9] *Individuals who provide opt-in consent typically have the right to opt-out of receiving such communications at any point after opting-in.*

[10] *GDPR Article 7(4). "Opt-in" consent is contrasted to "opt-out" consent where consent is presumed unless an individual specifically opts out."*

[11] *Id. Article 7.*

[12] *Id. Article 8-9.*

[13] *See, e.g., California Civil Code § 1798.82(h), defining "personal information" for purposes of data breach notification.*

[14] *Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 is a federal United States law which governs privacy and security of individuals' protected health information (PHI). See https://www.govinfo.gov/content/pkg/PLAW-104publ191/html/PLAW-104publ191.htm*

[15] *Gramm-Leach-Bliley contains privacy and security requirements enforced by the Federal Trade Commission. See https://www.ftc.gov/tips-advice/business-center/guidance/financial-institutions-customer-information-complying.*

[16] *The Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501-6505, is a federal United States law which governs the privacy of children under thirteen. It is administered by the Federal Trade Commission under the COPPA Rule, 16 CFR Part 312. See https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule*

[17] *Cal. Civ. Code §1798.140(o)(1).*

[18] *See, e.g., R. Disphan, House Hearing on Federal Privacy Law Takes Aim at GDPR, CCPA, https://www.law.com/legaltechnews/2019/02/26/house-hearing-on-federal-privacy-law-takes-aim-at-gdpr-ccpa*

[19] *For example, Article 5(1)(a) of the GDPR requires that personal data be "processed lawfully, fairly and in a transparent manner in relation to the data subject." Article 12 of the GDPR, requires controllers provide information and communications relating to processing to data subjects "in a concise, transparent, intelligible and easily accessible form, using clear and plain language....."*

[20] *https://iapp.org/news/a/transparency-and-the-gdpr-practical-guidance-and-interpretive-assistance-from-the-article-29-working-party*

[21] *In a recent case challenging the collection of geolocation information by the popular Weather application, the District Attorney's office in Los Angeles questioned the transparency of the data collection practices of the Weather Channel when those practices are buried in the midst of a 10,000 word privacy policy. https://arstechnica.com/tech-policy/2019/01/weather-channel-app-helped-advertisers-track-users-movements-lawsuit-says*

[22] *GDPR Article 4(5).*

[23] *See California Civil Code § 1798.140(a), (h) (definitions of "aggregate consumer information" and "deidentified."*

[24] *Sankei, Reunited Mr. Big is planning their first Japanese tour in this June (in Japanese) February 21, 2009*

[25] *Lennon changed the name of his group from the Quarrymen to the Beatles, an obvious homage to Holly's Crickets, after recording a cover of Holly's "That'll be the Day", the Quarrymen's first recording.*

[26] *Guralnick, Peter (2005). Dream Boogie: The Triumph of Sam Cooke. Little, Brown and Company. ISBN 0-316-37794-5.*

[27] *Authors' interview with Piero Giramonti.*

[28] *GDPR Article 6(f).*

[29] *Cal. Civil Code §§ 1798.120, 1798.135.*

[30] *https://www.billboard.com/articles/columns/music-festivals/6539009/music-festival-statistics-graphic*

[31] *Authors' interview with Miles Feinberg.*

[32] *Authors' interview with Piero Giramonti.*