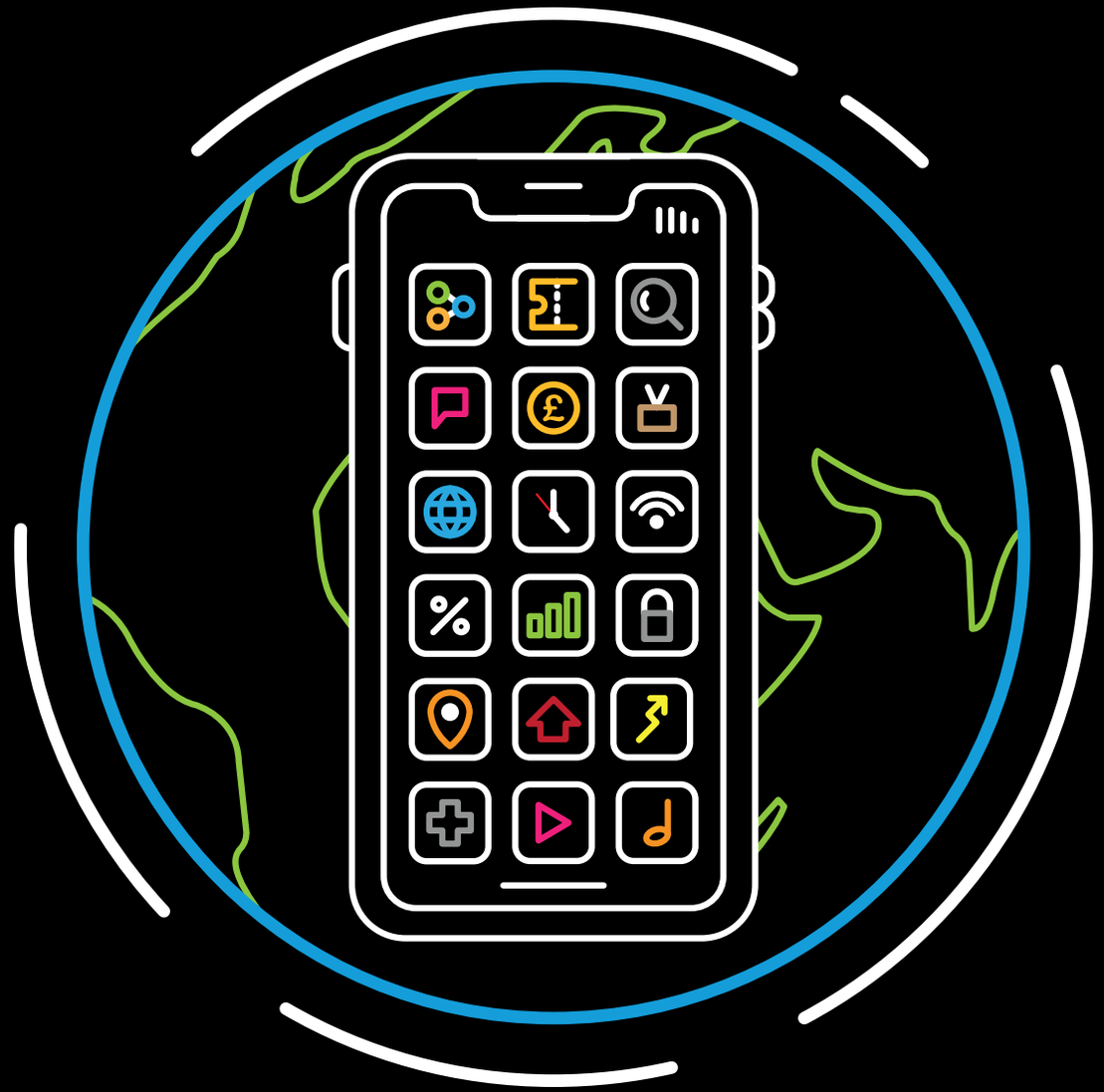
INTERNATIONAL ASSOCIATION OF ENTERTAINMENT LAWYERS

Nationalism vs globalism: regional and transnational legal issues reshaping the entertainment industry

Edited by William Genereux & Marijn Kingma



IAEL 2020

"Nationalism vs globalism: regional and transnational legal issues reshaping the entertainment industry"

Editors
William Genereux
Marijn Kingma

Publisher
FRUKT
www.wearefrukt.com

Design
Lauren Cotterell
Rashpal Amrit

Message from the President: Jeff Liebenson

I hoped this year of 2020 would be marked by our pursuit of this very interesting and relevant topic of Nationalism vs Globalism. And also my tenth year of serving as President of the IAEL, which is and continues to be such an honor.

But we are confronted by a pandemic that has affected our world. As we go inward to avoid mass contagion and yet continue to hear about its devastating effects across the globe, it sometimes is difficult to think of anything else. I echo the co-editors' hope that normalcy will to some degree return soon.

I am quite certain that the subject chosen by our co-editors will remain relevant. So in that spirit, we move on.

At times like this, it's inspiring to see the IAEL do what the IAEL does best—focusing on the key issues of the day, and enjoying the collegiality of our fellow members across national boundaries.

So while the world is going through distancing and isolation, the IAEL has come together to mount its first-ever digital IAEL Legal Summit. This has been a true group effort with major contributions from different corners of the world, bringing our different backgrounds and perspectives to work together across national borders.

I want to thank Marijn Kingma from The Netherlands and William Genereux from Canada, our co-editors who have brought their experiences from where they live and their legal expertise to life in developing this book, as well as our contributors for providing their rich perspectives.

Thanks to Duncan Calow and Marcel Bunders for your continued support, guidance and humor with respect to the many adversities we have weathered this year!

While the book focuses on digital and other entertainment deals crossing borders, it also addresses what legal needs still should be considered on a national or country-by-country basis. Our hope is that exploring these legal trends will help us in guiding our clients to deal with our multicultural world of entertainment law, notwithstanding the nationalistic urges of our time.

Perhaps this mirrors our staging of this digital IAEL Legal Summit with members from around the world enjoying our different cultures and coordinating our common interests.

We look forward to the upcoming publication of this, our 35th annual book published by the IAEL, Nationalism vs Globalism: Regional and Transnational Legal Issues Reshaping the Entertainment Industry.

Editors' Introduction:
William Genereux & Marijn Kingma

When this year's topic 'nationalism vs globalism' was chosen at the IAEL general meeting in 2019, no one could have foreseen that our world would soon be faced with a global pandemic. As we are writing this, COVID-19 has halted normal life throughout the world. With countries taking extreme lockdown measures, the impact on the economy is unimaginable and the entertainment industry had been brought to a near standstill. Concerts, festivals, movie releases and other events have been cancelled and entertainment lawyers are faced with unprecedented legal issues. But the entertainment industry is also proving its creativity in these times with initiatives like drive-in festivals, balcony concerts and virtual movie watching parties.

It was unavoidable that Midem, where we present our annual IAEL book each year, was cancelled. This has led to the decision to hold our 2020 IAEL book so that we can present it to the IAEL community at next year's Midem. The book will be released as the "IAEL 2020-2021" book. We believe the topic and content of the book will remain relevant.

However, we did not want to refrain from publishing anything at all this year, so we have decided to release five contributions from our book for next year as a 'sneak preview.' We believe the chapters we have chosen are a good reflection of our book and are also great standalone reads.

Our 2020-2021 book will explore the longstanding conflict between nationalism and globalism as it relates to the entertainment industry. Contributions will be subdivided into three major categories. The first category focuses on issues in specific jurisdictions and markets. The second attempts to map-out the expansion of regional forces into wider applications. The third seeks to bring a holistic view that reconciles many of the vital issues affecting the industry at large, and which are shaping our future world.

As a sneak preview from the first chapter, we have chosen a contribution about the effects of Brexit on the entertainment industry, a topic that cannot be missed in a chapter about regionalism. From the second part of our book, we have selected two articles about the effect of the GDPR around the world, as countries are adapting their data protection legislation to keep up with Europe's strict rules. Finally, we have released two contributions from the third chapter of the book. The first looks at the (im)possibility to regulate fake news and political advertising on social media platforms. The second article is about what is no doubt the biggest challenge of our times: global warming. The article discusses environmental impacts of recorded music and what we as lawyers can do to help mitigate climate change.

The fast spread of the virus is a direct result of globalization – international air traffic has quickly moved it around the world. And while countries are all imposing their own countermeasures, the virus knows no national borders. Meanwhile, globalization may also halt the virus. The global scientific community was able to find a reliable test for COVID-19 within days and is now working together to find a treatment and a vaccine. We are hoping that by the time our book comes out in 2021, global efforts will have resulted in a return back to – relative – normalcy.

We would like to thank IAEL's president Jeff Liebenson for his time, effort and leadership. We would also like to thank Janneke Popma, associate at Höcker, for her indispensable organizational skills. Additionally, the authors all need to be recognized for their creativity and their understanding when we had to postpone the release of the book.

Thank you everyone.

>> William Genereux

TORONTO

William is a Toronto lawyer with 35 years' experience in entertainment law, corporate law and litigation. In the 1980s he played in a hardcore punk band. In the 1990s he co-owned and operated a dance music record label. In the 2000s he was a lecturer at the Ted Rogers School of Management – Ryerson University, Toronto. His clients include top-selling recording artists, producers, writers, digital technology entrepreneurs and filmmakers. He is a member of the Law Society of Ontario, volunteers with Artists' Legal Aid Services in conjunction with the University of Toronto Faculty of Law, and is a past-chair of the Canadian Bar Association – Ontario, Entertainment, Media and Communications Law Section.

>> Marijn Kingma

U.S.A.

Marijn Kingma is a partner at Höcker Advocaten, based in Amsterdam. Marijn specializes in information law, with a focus on copyright and privacy-related issues. Marijn has a varied practice; her clients range from collective management organisations and NGO's to broadcasters and international entertainment companies. She conducts complex, strategic litigation and has been involved in several national and European landmark cases. Marijn is ranked in the Chambers guide as a "very strong, young up-and-coming lawyer" who is "unbelievably good and very clever" and is ranked in the Legal500 guide as "next generation lawyer", noting that "her knowledge, flexibility and positive mood makes working with her a fun, but still very effective experience". She is editor for the Dutch law journal AMI, an active member of the International Association of Entertainment Lawyers and a regular speaker at (national and international) conferences.

Who's your data? How new local privacy laws will frustrate the global music industry's data-driven growth

"Music businesses operating in the sea of data that is the new normal confront two opposing forces."

Authors: Tim Toohey and Bill Hochberg

Timothy Toohey is a partner at Greenberg Glusker LLP and based in Los Angeles, CA. An intellectual property lawyer as well as a privacy and data security attorney, Tim Toohey works hand-in-hand with organizations, entrepreneurs, and high-profile individuals—entertainers, actors, and athletes—on matters of data strategy and security, drawing upon his proven ability to translate technical aspects to non-technical persons. He helps his varied clients efficiently collect and secure the data and intellectual property crucial to their success in today's connected world. Tim is the head of the firm's Cybersecurity and Privacy practice. He is a U.S. Certified Information Privacy Professional, a European Union Certified Information Privacy Professional, and a Certified Information Privacy Manager.

Bill Hochberg heads the music department of Greenberg Glusker LLP, handling transactional and litigation matters for well-known and up-and-coming creative talents and their innovative companies, from monumental creators such as Bob Marley and Curtis Mayfield to top pop artists like Fifth Harmony and Britney Spears, and many in between. Bill writes on key music- and media-related topics for Forbes, the Atlantic, WIRED and other leading publications. He's frequently quoted in the media on the state of the music industry and how music law and technology can help artists and music companies become more successful going forward.

>> Introduction

Music businesses operating in the sea of data that is the new normal confront two opposing forces.

The big data urge.
The first is the urge to collect all manner of actionable personal data worldwide. If a little data is good, more data is better. This could be described as the big data urge where businesses aim to collect more and more personal data aspects and then combine it all in profitable ways. As algorithms improve and data scientists become more sophisticated, the big data urge chases the prospect of hitherto unforeseen connections.

A music festival like Coachella or Lollapalooza Paris may want to collect not only garden variety personal information, but a forest of data about throngs of concert goers. The range and type of such information are as wide as the preferences and tastes of music fans. In addition to traditional data points like name, address, gender, age, financial and health information, the definition of "personal information" in laws such as the European Union's "General Data Protection Regulation" (GDPR) and the California Consumer Privacy Act ("CCPA") now includes any information that can "directly or indirectly identify(an individual)." Information about location, biometrics, and interaction with social networks obviously comes to mind. But what about musical taste? Is this the new frontier of data?

Musical taste is not a closely guarded secret like, say, financial or physical health. But it has value to commercial data collectors, such as advertisers. "In the AdTech world they know they can detect the state of mind I'm in from the music I listen to and how I listen to it,"[1] says Karima Noren, co-founder of the UK-based Privacy Compliance Hub and a former Google inhouse attorney. "They want to know my mood so they know when is a good time to serve me with a particular ad." A music festival collecting information about concert goers is going to be interested in which performances a fan attended, the traits and likely preferences of that fan, the amount of time the fan spent viewing a show, what song was playing when the fan approached a stage (tracked with geofencing equipment), what song was playing when the fan moved from the stage to the exit, what refreshments the fan partook, among other things.

"The big data urge is closely allied with the internationalization of data."

Are all of these data points considered personal information according to data protection laws? Is there utility in combining the points to profile, and ultimately market things to, a population of fans who look alike in terms of the data they're throwing off? Do these data points (and the conclusions derived from them) cross national boundaries? Is it permissible under data protection law to combine data points from different individuals? Can information be combined from concert goers at different performances in different countries to gain insights into the difference of taste and fans' experiences in different locales? The answer is technically yes to all of these questions, but the permissibility of such actions depends on data protection laws in certain countries.

The *big data urge* is closely allied with the internationalization of data. As the music industry comes to operate more internationally, those who participate in the industry share data with branches and affiliates outside the country of origin of the data. For example, companies increasingly operate on a global scale. They also compete on a global scale and offer consumer benefits on a similar scale. A wide range of music is freely available through major streaming platforms in a variety of high resolution digital media. The music of relatively small countries, like South Korea and Jamaica, is widely available in ways that were unimaginable in the analog pre-Internet era, when fans would search out record stores with obscure "world music" sections to keep up with the latest Reggae or Korean Pop hit.. Today, artists have a broader marketplace for their music because of globalization and boundary-less digital distribution. Tastes have also expanded among fans who seek out new music internationally.

Leaving aside the perceived negatives of globalization, such as dominance of local and national companies by better funded global concerns), globalization also faces resistance from tough and resilient national and local companies, indigenous artistic tastes and unpredictable economics.

Data privacy law

In similar fashion, the international aspects of the big data urge face their own resistance by national and transnational privacy laws, data localization requirements, and prohibitions against international transfer of personal information.

By their very nature, data privacy laws—which protect personal information or personal data regarding individuals—are localized (even where, in the case of the European Union, "locality" is a multi-member union with certain uniform legislation, like the GDPR). In the case of the EU, the GDPR has established restrictions against the free flow of information in several respects.

First, the GDPR requires that companies wherever located, that collect personal information of EU residents (or "data subjects") have a legal ground for collection of personal data, such as "legitimate interests" (if these are not overridden by the interests or fundamental rights and freedoms of the data subject), explicit and freely given consent, or the necessity to fulfill a contractual commitment. Those data subjects are in turn granted certain rights regarding the data collected, including, in some instances, a right for deletion of the data. Moreover, the GDPR is based on the fact that the right to privacy in the EU is a fundamental right standing on a similar footing with freedom of expression. The privacy laws thus express a cultural preference within the EU for data privacy in ways that is not shared by all countries outside of the EU, such as the United States.

The right to be forgotten

For example, data subjects in the EU have the right under Article 17 of the GDPR "to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay under certain circumstances," including (a) where data is no longer relevant for the purposes for which they were collected; (b) the data subject has withdrawn consent; (c) the data subject objects to the processing, including profiling; (d) personal data were unlawfully processed; (e) the personal data has to be erased for compliance with a legal obligation.

The exercise of the "right to be forgotten" founded on pre-GDPR EU law potentially undermines what would be considered core values in other contexts and in other countries. For example, Europeans have used this right to remove certain information from Google's search results that would most likely be protected by freedom of the press in the United States. For example, the European Court of Justice upheld the request of a Spanish man—Mario Costeja Gonzalez—to remove a link to a story about the auction of his foreclosed home.[2] In Germany, lawyers for a convicted murderer had information

"The controversy over the right to be forgotten is not limited to search engines, such as Google."

from a Wikipedia article removed.[3] On the other hand, the EU's top court ruled in 2019 that Google only has to remove links from search results in Europe—and not globally.[4] In other words, Google is required to hide the page only from European search engine requests not international requests. The dispute arose between Google and the French privacy regulator, who argued that Google had to delist results globally and not just within the EU. (In the briefing of the issue Google stated that it had received more than 845,000 requests to remove a total of 3.3 million web addresses with about 45% of the links ultimately getting delisted.) There are very significant consequences for companies like Google for not removing data. The Swedish Data Protection Authority (DPA) recently fined Google with a 75 million kronor ($8 million) fine for failing to comply with the GDPR when it allegedly failed properly and promptly to remove search results under the GDPR's right-to-be-forgotten requirements.[5]

The controversy over the right to be forgotten is not limited to search engines, such as Google. For example, a European data subject aggrieved by the unauthorized collection of personal information at a music festival may bring an action or make a complaint to the relevant data protection authority to have that information removed. Depending on the nature of the data gathered by the festival and the identifiers attached to such data, it may be logistically difficult for the festival to remove a single bit of data or, if it is a music festival outside of the EU, to identify the data that pertains to EU residents (as opposed to other individuals in the database). The removal of data may threaten the viability of the data set as well as integrity of such data if anonymized data (i.e., data without personal information) cannot meet the requisite purposes. The festival may also incur substantial costs in complying with rights from EU residents. Under the recent Swedish DPA ruling, the holder of the data may even get in trouble if it notifies the website owner in advance about removal on the ground that this may give the website owner an opportunity to move the data to another website.

Data privacy laws outside of the EU

The challenges of localized privacy laws has become even more acute as individual states in the United States have enacted laws giving their "consumers" enhanced rights that residents in other states do not have. For example, California's Consumer Privacy Act (or "CCPA"), gives Californians the right to (1) know what personal information is being collected about them and who is buying it, (2) easily opt out, and (3) get equal service and price, regardless of whether they opted out.

CCPA and GDPR, along with other laws in India and elsewhere, could impact the music industry. For example, music festivals can be restricted in use of fan data to sell sponsorships to brands desiring to position logos on stages in front of certain crowds. Artists, too, could be restricted. They may no longer be able to use "geo-fencing" location data to see which songs draw fans toward the stage and which drive them toward the exit, when the data concerns EU or California data subjects. And music publishers who have used social media numbers to pitch tunes for car commercials, as well as record labels who have relied on data for A&R purposes are impacted.

The California law, effective January 1, 2020, applies to companies with revenues of US $25 million or more, ones that gather data on at least 50,000 California users, or those making more than half of their money from user data transactions.

California's larger fests like Coachella, with some 90,000 attendees per day, and Outside Lands (200,000 total) are certainly impacted by the new law, yet smaller ones like Kaboo (40,000 fans) and Lightning in a Bottle (20,000) may believe they're exempt, at least when it comes to data they collect from radio frequency ID wristbands that track fans' movements and purchases. Likewise, small record labels - often labors of love - may believe they can slip through the netting of CCPA because the law targets bigger fish.

"This is going to be the year of big fines," says Noren, "including against small companies. All it takes are a few customer complaints to trigger legal action."[6] Recent fines under the GDPR, such as the Swedish DPA's action against Google and a €50 million fine against Google by the French data protection authority for lack of transparency under the GDPR[7] , shows that this is a reality.

In addition, London-based Urban Massage is facing fines of up to 4% of its gross revenue for allegedly violating the GDPR for using data about clients' names, contact information, massage preferences, and even alleged sexual activity.

"Data localization laws may prevent free flow of data for companies operating across borders."

GDPR penalties can rise as high €20 million (about $22.3 million) or up to 4% of worldwide gross revenue for egregious violations. But the penalties are supposed to be proportionate to the violation. By comparison, the CCPA statutory penalties are smaller, with a $7500 fine for intentional acts and $2500 for non-intentional ones. But it is currently unclear how those fines will apply.

The state of California is expected to roll out regulations to make it clearer whether the CCPA fines are assessed per infraction or per affected user. In other words, we don't know yet whether it will be treated as one violation with a $7,500 fine or 50,000 violations with penalties ranging up to tens or even hundreds of millions for a website or app with many users. This remains unknown until the final regulations will be published by the California Attorney General. Companies operating outside California or the E.U. are not immune to these privacy laws, which can still apply if customers are residents of those jurisdiction

The laws don't stop state surveillance or curtail cops from tailing criminals, but could crimp "surveillance capitalism." The U.S. Drug Enforcement Agency, for instance, could still stake out a meth dealer who listens to death metal at 4 a.m. to know when not to raid, but a drug company can't target him for sleep aids, and a criminal defense firm can't serve him with an ad for a criminal defense law firm based on his personal data or profile under US law.

Data localization laws

The tension between globalization and localization in data protection is also exhibited in data localization laws. The GDPR does not prohibit transfer of data outside of the EU, but does require that the transfer be to a jurisdiction that provides an "adequate level" of data protection. For example, the European Commission has determined that Japan, Israel, Argentina, New Zealand, Switzerland and several other countries have a comparable level of protection for personal information as do countries in the European Union. The United States and Australia (to take just two examples) are not deemed "adequate." For example, the United States does not have a comprehensive privacy law similar to the GDPR. Data transfers to the United States are nonetheless allowed under certain circumstances under the Privacy Shield mechanism (administered by the US Department of Commerce) and other mechanisms, such as Binding Corporate Rules.

More extreme are "data localization laws" that require data to be processed in a particular territory. These laws, which are motivated by security and protectionist concerns, may prevent businesses from using the cloud—or require that the cloud servers be located in a particular location. Examples of such laws (which may pertain only to certain types of data) include those of Russia and China (and other countries in the Asia-Pacific region) for personal data.

Data localization laws may prevent free flow of data for companies operating across borders. Such laws may even give businesses second thoughts about conducting events in certain jurisdictions, particularly those (such as China) that engage in protectionist concerns for cultural and artistic proceedings.

India, in a more extreme instance, has passed legislation that not only requires data localization to the extent that the Indian government keeps a copy of the data, but also gives Indian law enforcement the right to un-encrypt messages between users on Facebook, WhatsApp and other services with messaging functions that are sold to the public as private and secure.

Such legislation will likely lead to a balkanization effect, as more and more countries around the globe, and large states within countries such as California, promulgate rules for both domestic companies and multinationals that do business in their territories that could severely impact privacy, protection, and speech rights and expectations. How this shakes out for the music industry, and whether digital commerce and concert attendance slows in more restrictive data-flow territories, has yet to be determined.

[1] *Bill Hochberg, The Music Biz Is Addicted to Data and the new privacy laws may make it go to rehab, Forbes January 1, 2020, available at https://www.forbes.com/sites/williamhochberg/2020/01/16/the-music-biz-is-addicted-to-data--and-new-privacy-laws-may-make-it-go-to-rehab/#32d3fdd03f86.*

[2] *Court of Justice of the European Union, 13 May 2014, Case No. C-131/32 (Google Spain), available at http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&doclang=EN.*

[3] *See https://www.theguardian.com/world/2019/nov/28/german-court-backs-murderers-right-to-be-forgotten-online.*

[4] *Court of Justice of the European Union, 24 September 2019, Case No. C 507/17 (Google LLC), available at http://curia.europa.eu/juris/liste.jsf?language=en&num=C-507/17.'*

[5] *See https://www.datainspektionen.se/nyheter/the-swedish-data-protection-authority-imposes-administrative-fine-on-google/.*

[6] *Bill Hochberg, The Music Biz Is Addicted to Data and the new privacy laws may make it go to rehab, Forbes January 1, 2020, available at https://www.forbes.com/sites/williamhochberg/2020/01/16/the-music-biz-is-addicted-to-data--and-new-privacy-laws-may-make-it-go-to-rehab/#32d3fdd03f86.*

[7] *See https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc.*