Stanford – Vienna
Transatlantic Technology Law Forum

A joint initiative of
Stanford Law School and the University of Vienna School of Law

Transatlantic Antitrust and IPR Developments

Issue No. 1/2024 (October 24, 2024)

Contributors:

Alexandros Kazimirov,
Fabien Lechevalier,
Marie-Andrée Weiss

Editor-in-chief: Juha Vesala

Editor: Runhua Wang

Contents

About the contributors

Alexandros Kazimirov is a Research Fellow at the American Antitrust Institute. His research scrutinizes the repercussions of artificial intelligence startups being subsumed by tech incumbents through quasi-mergers and examines the adequacy of the regulatory response in terms of emerging market dynamics. He graduated from Berkeley Law School. While in law school, he clerked at the European Court of Justice. After taking the attorney's oath, he was appointed a Transatlantic Technology Law Forum Fellow at Stanford Law School. He is a member of the California State and American Bar Associations. He serves on the Board of Advisors of the SEC Historical Society.

Fabien Lechevalier is a Ph.D candidate in Law & Economics at Paris-Saclay University, France. He is a researcher at the Center for Studies and Research in **IP/IT** Law (CERDI) in France and at the International Observatory on the Societal Impacts of AI and Digital Technology (OBVIA) in Canada. His research focuses on the collective dimension of the right to informational privacy, collective models of personal data governance and design research methods applied to law. With a multidisciplinary background, at the crossroads of law, economics and design, he is interested in research-action and research-creation approaches in the legal environment. He was a Visiting Fellow at the Digital Life Initiative at Cornell Tech, and is a member of the NYU Privacy Research Group. He is a Lecturer in law at the Jean Monnet Faculty of Law-Economics & Management, Paris-Saclay University and at the Mines-Telecom School of Engineering and Management. He currently co-pilots the Lab Surveillance, an experimental lab for legal research through design, supported by ENSCI Design School and Paris-Saclay University. He joined the TTLF as a TTLF Fellow in 2024.

Marie-Andrée Weiss is an attorney admitted in New York and in Strasbourg, France (inactive in France). Before becoming an attorney, she worked for several years in the fashion and cosmetics industry in New York as a buyer and a director of sales and marketing. She graduated from the University of Strasbourg in France with an M.A. in Art History, a J.D. in Business Law, an LL.M. in Criminal Law, and an LL.M. in Multimedia Law. Marie-Andrée also graduated from the Benjamin N. Cardozo School of Law in New York City with an LL.M. in Intellectual Property Law. She is an attorney in New York and her solo practice focuses on intellectual property, privacy, data protection, and social media law.

Intellectual Property
United States

NO FAKES Act Bill: Toward a Federal Right of Publicity Law?

By Marie-Andrée Weiss

The bipartisan Nurture Originals, Foster Art, and Keep Entertainment Safe Act (NO FAKES Act) bill was introduced in the U.S. Senate the last day of July 2024 and the House of Representatives on September 12, 2024. A draft of the bill had been published in October 2023 and a hearing about it took place last April in the Senate Judiciary Subcommittee on Intellectual Property.

The NO FAKES Act would protect privacy and property rights. It aims at protecting the voice and visual likeness of any individual, famous or not, whether they commercialize their likeness or not. It would thus generally protect individuals' right to privacy and even their honor, as their likeness may be used to create false or obscene deepfakes.

However, the law would also allow all individuals to profit commercially from their digital replicas during their lifetime. As such, the law would be the first federal right of publicity law, a domain thus far only regulated by states in the U.S. and would even preempt any cause of action under some U.S. state laws protecting the voice or likeness or an individual.

The right would be transmissible upon death, and heirs would have to register their rights in an ad hoc registry held by the U.S. Copyright Office. Digital replicas of deceased individuals would be somewhat similar to works protected by copyright, but fair use would not be a possible defense for their unauthorized use, as the bill does not provide for such right.

What is a digital replica?

The bill broadly defines a "*digital replica"* as:

"a newly created, computer-generated, highly realistic electronic representation that is readily identifiable as the voice or visual likeness of an individual that:

(A) is embodied in a sound recording, image, audiovisual work, including an audiovisual work that does not have any accompanying sounds, or transmission (i) in which the actual individual did not actually perform or appear; or (ii) that is a version of a sound recording, image, or audiovisual work in which the actual individual did perform or appear, in which the fundamental character of the performance or appearance has been materially altered; and

(B) does not include the electronic reproduction, use of a sample of one sound recording or audiovisual work into another, remixing, mastering, or digital remastering of

a sound recording or audiovisual work authorized by the copyright holder."

Senator Thillis played during his opening statement in the April hearing a song from Drake, which sounded like it was sung by Tupac Shakur, who died several decades ago (the estate of Tupac Shakur threatened to sue Drake). This is one of many examples of a digital replica who would be protected by the new law. Other examples are more sinister, as "deepfakes" are performing fake acts, including sexual acts, or saying things that were not said by the real person, such as a deepfake of President Biden telling voters not to vote in a primary election.

A property right which can only be licensed or sold after the death of the individual

The "right holder" of the "digital replica" is the person whose voice or visual likeness is embodied in such digital replica, or the person holding such right, either through a license, acquisition, or inheritance. Indeed, the rights in the digital replica could be sold and bought, and the NO FAKES Act would specifically authorize it, under certain conditions.

During the lifetime of the individual, it is an exclusive property right, which can be licensed, in whole or in part, only by the individual. However, it cannot be sold. It could be bequeathed by a will to heirs, and, upon the death of the individual, the executors, heirs or assigns could transfer or license it. The post-mortem right would be exclusive to the right holder for 10 years following the individual's death.

The Copyright Office would maintain a directory of post-mortem digital replication rights, available online. Registration in this directory would not be mandatory during the initial 10-year period but would be mandatory 10 years after the death of the individual whose likeness is digitalized.

A right which could be held 70 years after the death of the individual provided that it is renewed every 5 years

After the 10-year initial period expires, protection could be extended by 5 years increments. The renewal of this post-mortem right would only be effective if the right holder files a notice with the Register of Copyright and provides a sworn statement confirming that the right holder has been actively engaged in an authorized public use of the individual's voice or visual likeness during the 2-year period preceding the current period's expiration.

The requirements for the license

The NO FAKES Act distinguishes licenses granted by the individual from post-mortem licenses.

All Licenses granted by individuals during their lifetime would have to be in writing and

include "*a reasonably specific description of the intended uses of the… digital replica*." Licenses granted by individuals at least 18 years old could not exceed 10 years and must be signed by the individuals. If the individual is a minor, the license could not exceed 5 years and would terminate when the individual turns 18. It would have to be approved by a competent state court.

Licenses granted postmortem must be in writing and signed by the right holders or their authorized representatives.

Liability for using the digital replicas without authorization

It would be a civil liability to produce a digital replica without the consent of the applicable right holder, or to publish, reproduce, display, distribute, transmit, or otherwise make available such replica to the public.

To be liable, the person would have to have actual knowledge of the right, which could be acquired by receiving a notification of the right holder or if the person would "*willfully avoid having such knowledge.*" The bill does not specify what could be such willful avoidance, but one can imagine, that claiming that one does not know that Prince or Kobe Bryant have been dead for less than 10 years would be considered willful avoidance. However, whether the person could successfully argue that it did not know that the right was registered could relate to how much the public becomes aware of such register.

A right to use digital replica freely in the news

The bill specifies that using digital replicas would be authorized for news and broadcast purposes, or for use in a documentary or a biography, even if this entails "*some degree of functionalization*," provided, however, that such digital replica does not create "*the false impression that the work is an authentic sound recording, image, transmission, or audiovisual work in which the individual participated.*"

It would not be legal to embody the digital replica "*in a musical sound recording that is synchronized to accompany a motion picture or other audiovisual work*," unless such use of the digital replica is protected by the First Amendment to the Constitution.

This specifically addresses the issue of "deep fakes" being created to appear to be an actor or a musician, as in Drake's song. A digital replica could also be produced or used for bona fide commentary, criticism, satire, or parody or if its use is "*fleeting or negligible.*"

Safe Harbor & Notice and Take Down

The law would be considered as pertaining to intellectual property for the purpose of Section 230 of the Communication Act and thus online service providers would not be protected by this immunity, since it does not apply to intellectual property lawsuits.

Online service providers would, however, be protected by a safe harbor for storing illegal digital replicas if they remove or disable access to them "*as soon as is technically and practically feasible*" after having been notified. They also would have to promptly notify the third party that provided the material that it has been removed or disabled. This is similar to the Digital Millennium Copyright Act (DMCA) notice and take down scheme. However, unlike the DMCA, the NO FAKES Act would not allow the person who posted the allegedly illegal digital replica to send a counter-notice to try to have the content restored, as is possible under the DMCA, and thus the law would likely be used to chill speech.

Liability

If enacted, the NO FAKES Act would have to be taken seriously, as violators of the law would be liable for fines and actual damages and could also have to disgorge their profits attributable to such illegal use.

Several groups have expressed their objections, including the Computer & Communications Industry Association and the American Library Association, concerned that the law could be used as a "heckler's veto," that the persons could become "*alienated from their own likeness*" and would generally encumber free speech. The NO FAKES Act is likely to face a rough road ahead before, if ever, becoming law.

Other Developments
United States

Artificial Intelligence and the Regulator's Dilemma

By Alexandros Kazimirov

On September 9, 2024 the Safe and Secure Innovation for Frontier Artificial Intelligence Models Act (SB 1047) reached the office of the Governor of California after passing the State's Assembly and Senate. Three weeks later, he vetoed it. Recognizing the rapid pace of advances in artificial intelligence, the bill attempted to introduce certain safety precautions and regulatory oversight for frontier model developers. This piece addresses certain points of discourse about SB 1047.

1. Safety testing and assessment of capability to cause or materially enable a critical harm[1]

Sometimes, text too difficult to construe may entail lack of fair notice to regulated entities. In its letter opposing the bill, Meta claimed that "there are no existing benchmarks for the types of AI safety testing that the bill contemplates." Unlike crypto regulation, vagueness hardly applied here. Even if SB 1047 did not describe the specific mechanisms, the bill defined the threats that it sought to prevent.[2] This way, SB 1047 incentivized developers to commit resources to robust safety controls. This approach allowed a degree of institutional durability. It made the text adaptable through subsequent adjustments, without making it too prescriptive.[3] In turn, adaptability ensured that the statute would remain relevant as the technology evolved. And to the extent that a company had already acted on its commitments to develop safety and security protocols, compliance costs may have been partly mitigated if they built on such pre-existing measures.

2. New barriers to entry

Unlike crypto regulation which imposed reporting and registration requirements without setting thresholds, SB 1047 had a clear scope.[4] SB 1047 imposed costs primarily on large model developers instead of smaller startups or solo coders. And if these thresholds became obsolete because developers improved the efficiency by curating their models with better quality - rather than sheer mass - of information, then the statute

[1] Sec. 22603(a)(3)(C)(i) and 22603(b)(1).
[2] Sec. 22602(g)(1).
[3] Anthropic's letter at p. 4.
[4] Sec. 22602(e)(1)(A)(i).

retained mechanisms to "redefine the compute thresholds that trigger the law's safety requirements."

3. Costs on secondary users

Unlike crypto regulation which did not differentiate between core developers and subsequent user interface and client software developers, SB 1047 distinguished between foundation model developers and those who engage in fine-tuning of frontier models. Further, SB 1047 set compute thresholds for what level of fine-tuning was acceptable before a model would be substantially transformed and liability attached.[5]

4. Enforcement

SB 1047 limited the cause of action to be enforceable only by California's attorney general, thus avoiding the incentive for private plaintiffs to sue developers. Liability was proportional to a company's (i) commitment to allocating resources and developing safety and security protocols, (ii) corporate governance controls and whistleblower protections and (iii) good faith conduct.[6] It would have been counterintuitive to expect the attorney general to pursue zealous enforcement while the technology is still subject to vast improvement. It seems plausible that the purpose of SB 1047 was to put in place certain guardrails before the technology matured and, in the meantime, allow the attorney general to exercise his role with discretion.

5. Worse than the EU AI Act

Compared to the EU AI Act, SB 1047 set more concrete standards and enforcement mechanisms which depending on enforcement policy, may indeed have resulted in a stricter regime. However, SB 1047 was narrower in scope due to its clear thresholds and enforcement would have probably been lax while the technology developed.

6. Preference for federal regulation

In its letter opposing the bill, OpenAI claimed that federal legislation is more efficient to regulate the industry. However, in the absence of an AI Act by Congress in the foreseeable future, SB 1047 could have served as a first step in standard setting. Further, as with environmental protections, the federalist model of governance allows California to impose stricter policies.[7]

[5] Sec. 22602(e)(1)(A)(ii).
[6] Sec. 22607.
[7] Sec. 22609.

7. Risk to open source

To be sure, SB 1047 increased the burdens on model developers pertaining to their open-source models. This may have had negative repercussions for the developer community relying on open source. However, even with SB 1047 now off the table, there is no guarantee that there will be no attempts to commercialize open source or leverage the open-source community to protect closed-source projects.

8. Necessity and proportionality

The urgency of reforms is tied to the underlying visions of artificial intelligence that people carry. To skeptics, regulation is imperative. To enthusiasts, it is not. Compared to blockchain, the potential risks arising from the scope and speed of impact are significantly greater. Statements by CEOs of major tech companies all recognize the threats of unchecked advancements in this field. At least compared to crypto regulation, the world seems to agree that the need to regulate artificial intelligence is much more urgent.

9. Public scrutiny

Unlike crypto regulation, overall (i) a prolonged period of consultation with stakeholders, (ii) heightened participation and public feedback, (iii) consecutive revisions of the text, and (iv) intense scrutiny of the statute illustrated an open administrative process with receptive lawmakers.

10. Conclusion

Because artificial intelligence is progressing so quickly, some rally for regulation, while others oppose it. Both sides have valid concerns. In this predicament, the regulator's dilemma means weighing the risk of impeding the prospect of innovation in the long term against the risk of allowing public harm to occur in the short term. Maybe SB 1047 was a measured first step which offered certain adjustable protections without being draconian. Maybe not, and that is why it did not become law. In sum, there is probably a preference for piecemeal legislation and low-profile, low-harm initiatives.

Other Developments

European Union

Should There Be a "Buy European [Tech.] Act" for Digital Services?

By Fabien Lechevalier

Despite the EU's recent adoption of a mechanism to ensure reciprocity in access to public procurement markets, political calls for establishing a "European preference" have paradoxically increased during the latest European elections. Concerns have arisen over the relative weakness of European offerings compared to foreign competitors. The idea of introducing criteria in public procurement based on the location of production or the nationality of the bidder is appealing. Often presented as a form of industrial policy, it could provide European companies with steady demand, enabling them to scale up, reduce average costs, and encourage investment.

Protecting Europe's Tech Industry

There is widespread concern over the absence of digital champions in Europe and the dominance of large American firms in the online advertising and data storage markets. While the European Union (EU) has taken steps, including regulations like the General Data Protection Regulation (GDPR) of 2016, the Digital Market Act (DMA) of 2022, and the Digital Service Act (DSA) of 2022, and strengthened competition oversight, its financial tools to support businesses remain limited. Some see a "Buy European Act" for digital services as a way to address the weakness of European market shares. Economically, such an act aligns with desires for a more protective Europe and supports the European digital industry. However, it is a point of contention among EU member states. Countries like Germany and Sweden, which value free competition, are wary of protectionist measures, fearing retaliatory actions from the EU's trading partners that could harm European businesses.

A European "Buy American Act"?

The comparison to the United State (U.S.) Buy American Act is often cited in support of implementing a similar approach in Europe, especially given the role of public procurement in the growth of certain network infrastructure sectors. The U.S. has various laws at both federal and state levels that favor domestic companies in public procurement. For instance, specific laws require that the Department of Defense (DOD) procurements are almost exclusively American (10 U.S.C. § 4862 and § 4863). More generally, the Buy American Act of 1933, the Buy America Act of 1982, and the Small Business Act of 1957 ensure that American companies or those based in the U.S. receive

preferential treatment in public contracts. The latter act also mandates that low-value contracts are reserved for small businesses if at least two can bid. However, there is little quantitative evaluation of the impact of these policies, making it difficult to fully assess their effects, though the Buy American Act likely supports American businesses through public procurement.

A political publicity stunt?

In Europe, there is now a broader consensus on the issue of sovereignty than there has been in the past regarding other dominant positions, such as in banking services (SWIFT, VISA). The COVID-19 crisis raised awareness of digital vulnerability, much like the Iranian crisis did for banking vulnerability and the Russian crisis for energy vulnerability. After crises, actors are often criticized for a lack of foresight. The call for sovereignty is more widely accepted when it comes to digital services. However, there are noticeable inconsistencies between political rhetoric and administrative actions, whether due to political realism or laziness. In France, for example, despite the launch of GaiaX, the European cloud services platform, the French government chose Microsoft's Azure Cloud over OVH for managing the COVID-19 epidemic monitoring application and storing health data, while BPI France (the French Public Investment Bank) used AWS services for managing state-guaranteed loans. This illustrates not just political inconsistency but also the challenge of imposing industrial policy goals on public procurement due to differing timelines, highlighting the need to clarify the relationship between these two policies when necessary.

Legal obstacles at the EU level

Within the EU, public procurement is governed by various legal texts, beginning with the Treaty on the Functioning of the European Union (TFEU). This treaty enforces principles of transparency, equal treatment, and non-discrimination in public procurement. EU directives, such as Directive 2014/24/EU, set minimum harmonization rules for the procurement of goods, works, and services by public authorities. Article 18 of this directive emphasizes the non-discrimination principle, prohibiting any artificial restriction of competition aimed at unfairly favoring or disadvantaging specific economic operators, for example, based on their nationality. This principle has been reinforced by the Court of Justice of the European Union (CJEU). The directive excludes certain sectors, such as water, energy, transport, postal services, defense, and security, which are covered by other directives (e.g., Directive 2014/25/EU and Directive 2009/81/EC) that also uphold the principle of non-discrimination. Exceptions exist only for extremely sensitive sectors, like intelligence services (Article 13 of Directive 2009/81/EC). These EU directives are transposed into national laws and apply to tenders exceeding specific monetary thresholds.

Legal obstacles at the international level

Internationally, the main treaty concerning public procurement is the Agreement on Government Procurement (GPA), which opens the EU's public procurement markets to the parties involved. The GPA, signed under the World Trade Organization in 2012, enshrines the principle of non-discrimination. This principle requires each participating state to provide goods, services, and suppliers from other parties with treatment no less favorable than that accorded to its own or other states' suppliers. Therefore, within the EU, operators from third countries must be treated similarly to those from EU member states. This is codified in Article 25 of Directive 2014/24/EU. The GPA applies to contracts above certain thresholds, which are relatively low (€5,382,000 for works contracts and €140,000 or €215,000 for supplies and services contracts). The adoption of a European measure that would contradict the GPA to limit access to public procurement markets seems unlikely. While the GPA does allow for exceptions, any such measures must not result in arbitrary or unjustifiable discrimination or create disguised restrictions on international trade.

Conclusion

It appears that beyond legal obstacles, it is difficult to assign public procurement a role in industrial policy because the timelines of these policies differ. Public procurement must meet immediate needs, which is incompatible with the long-term investment logic of industrial policy. However, over the past 10 years, policies have become more attuned to sovereignty issues in certain digital services and have made progress in developing a regulatory framework aimed at mitigating risks and guiding the allocation of digital contracts by public administrations. Nonetheless, beyond the requirement for reciprocity, the implementation of a national bias in favor of European actors has not been clearly established. While there are signs of digital protectionism through legal and regulatory measures, local preference policies motivated by environmental concerns have been more successful at the European level. In the digital sector, the "Brussels effect" may provide a competitive advantage to European players. Thus, industrial policy seems better suited to promoting technological innovation and achieving competitive advantages than enforcing a local preference principle. Compared to the current situation, the economic gain from market protection is far less than the political cost of European discord.

To learn more, please consult the report produced by the Digital, Governance & Sovereignty Chair of the School of Public Affairs at Sciences Po Paris (S. GUILLOU, F. G'SELL, F. LECHEVALIER):

https://www.sciencespo.fr/public/chaire-numerique/2024/06/06/rapport-buy-european-tech-act/

Copyright © 2024 contributors. This issue and the previous issues of the Transatlantic Antitrust and IPR Developments can be accessed via its webpage on the Transatlantic Technology Law Forum website.