COMPARING "DEEPFAKE" REGULATORY REGIMES IN THE UNITED STATES, THE EUROPEAN UNION, AND CHINA

Yinuo Geng*

CITE AS: 7 GEO. L. TECH. REV. 157 (2023)

TABLE OF CONTENTS

Introduction 157
I. Clarifying Existing Regulatory Proposals for Deepfakes 162
A. The United States' Approach 162
B. The European Union's Approach 165
C. China's Approach 167
II. Articulating Similarities and Differences Across the Three Jurisdictions 171
A. Regulating Specific Stages Along the Deepfake Lifecycle 171
B. Regulating by Sector or Risk Assessment 173
C. Regulating Individually or as Part of a Holistic AI Strategy 174
III. Learning From Each Other to Reach Outcomes-Based Regulations 176
Conclusion 177

INTRODUCTION

With increasing regulatory attention on digital technologies, it has become clear that the United States, the European Union, and China are all, concurrently and in parallel, developing rules and frameworks on how best to govern emerging technologies and set standards of acceptable technological

* Fellow, Georgetown Law Center on National Security; Master of Law and Technology, Georgetown University Law Center; M.A., International Economics and International Relations, Johns Hopkins University – Paul H. Nitze School of Advance International Studies. She also has over a decade of professional experience in the private sector advising business and technology leaders on aspects of technology strategy

use. Despite the seemingly borderless nature of technology, all three jurisdictions have sought to propose and implement a flurry of laws and regulations to manage digital technologies, as well as to limit the uneasy power held by technology companies. In recent months, the specific technology of "deepfakes" have risen to the forefront of regulatory scrutiny.[1]

"Deepfakes" can be defined as the use of AI techniques (such as machine and deep learning and, more specifically, Generative Adversarial Networks) to generate synthetic but exceedingly realistic video and audio media, especially of human facial and vocal likeness.[2] Deepfakes are used infamously in pornography, particularly nonconsensual and revenge porn, but also increasingly in political situations as well as for entertainment and educational purposes.[3] The technology is increasingly available for experimentation by anyone with a modicum of technical ability. Although truly high-quality deepfakes tend to require a large repository of images and/or videos, even low-quality deepfakes have the capacity to be very harmful. While there are notable positive uses,[4] the negative impacts are particularly

---

[1] Paul Mozur et al., *A Global Tipping Point for Reining In Tech Has Arrived*, N.Y. TIMES (Apr. 30, 2021), https://www.nytimes.com/2021/04/20/technology/global-tipping-point-tech.html [https://perma.cc/7HMU-7Q7M].
see Charles Q. Choi, *AI Creates Fake Obama*, IEEE SPECTRUM (July 12, 2017), https://spectrum.ieee.org/techtalk/robotics/artificial-intelligence/ai-creates-fake-obama [https://perma.cc/M6GP-TNZ4].

[2] A generative adversarial network (GAN) leverages two neural networks simultaneously, one to produce something that mimics a given dataset and the other to attempt to assess how successful the mimicry is. *See* Danielle K. Citron & Robert Chesney, *Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security*, 107 CALIF. L. REV. 1753 (2019); Ian J. Goodfellow et al., *Generative Adversarial Nets* (June 10, 2014), (Neural Information Processing Systems conference paper), https://arxiv.org/abs/1406.2661 [https://perma.cc/97SH-H7DD]; *See* Dave Johnson, *What is a deepfake? Everything you need to know about the IA-powered fake media*, BUS. INSIDER (Jan. 22, 2021), https://www.businessinsider.com/what-is-deepfake [https://perma.cc/5LPQ-PH53].

[3] Karen Hao, *Deepfake porn is ruining women's lives. Now the law may finally ban it,* MIT TECH. REV. (Feb. 12, 2021), https://www.technologyreview.com/2021/02/12/1018222/deepfake-revenge-porn-coming-ban/ [https://perma.cc/ZFR7-KGTF]; *See* Rob Toews, *Deepfakes Are Going to Wreak Havoc on Society. We Are Not Prepared*, FORBES (May 25, 2020), https://www.forbes.com/sites/robtoews/2020/05/25/deepfakes-are-going-to wreak-havoc-on-society-we-are-not-prepared/ [https://perma.cc/YDC6-FJNE] (One report found that 96% of deepfake videos found online in 2019 was pornography); Simon Parkin, *The rise of the deepfake and the threat to democracy*, GUARDIAN (Jun. 22, 2019), https://www.theguardian.com/technology/ng-interactive/2019/jun/22/the rise-of-the-deepfake-and-the-threat-to-democracy [https://perma.cc/FU4K-DKN3].

[4] Examples include: editing video without reshooting, experiencing things that no longer exist such as in a museum, increasing accessibility for individuals with disabilities (such as navigating an unfamiliar terrain for those with visual impairments), enabling better medical practices by creating "fake" scans, etc. *See* Simon Chandler, *Why Deepfakes Are A Net*

significant and highly visible, including emotional harm, identity theft, intimidation and harassment, reputational damage, political manipulation, and the undermining of trust.[5] There are also potential gray areas: for example, the use of deepfakes of celebrities in advertisements and training videos, with or without the celebrities' permission, has drawn scrutiny for ethical reasons yet it has also drawn interest by media and marketing firms for the ability to increase production at lower costs.[6]

Fears and concerns about deepfakes are driven by the potential for substantial harm, especially when they can be used to manipulate people into believing an individual said or did something that they did not. The goal can be to embarrass and silence critics; for example, the Indian investigative journalist Rana Ayyub was the subject of deepfake porn videos in efforts to discredit her work.[7] The technology is also a problem in political and electoral contexts. Recent months have seen the distribution of an altered video of Nancy Pelosi where she appears drunk and incompetent,[8] and a deepfake video where Ukrainian president Volodymyr Zelensky asks Ukrainian troops

Positive for Humanity, FORBES (Mar. 9, 2020), https://www.forbes.com/sites/simonchandler/2020/03/09/why-deepfakes-are-a-net-positive-for-humanity [https://perma.cc/6EP7-RJTW]; Ashish Jaiman, *Positive Use Cases of Synthetic Media (aka Deepfakes)*, TOWARD DATA SCI. (Aug. 14, 2020), https://towardsdatascience.com/positive-use-cases-of-deepfakes-49f510056387 [https://perma.cc/CW37-GLF3].

[5] The Panel for the Future of Science and Technology, part of the European Parliamentary Research Service within the Secretariat of the European Parliament, recognized three categories of harm associated with deepfakes: psychological harms, financial harms, societal harms; *see* EUR. PARLIAMENTARY RSCH. SERV., TACKLING DEEPFAKES IN EUROPEAN POLICY IV (Jul. 2021); Nicholas Diakopoulos and Deborah Johnson noted five types of harms in an electoral context: deception, intimidation, reputation, misattribution, and undermining trust; *see* Nicholas Diakopoulos & Deborah Johnson, *Anticipating and Addressing the Ethical Implications of Deepfakes in the Context of Elections*, 23 NEW MEDIA & SOC'Y 2072 (2020) [https://perma.cc/5M5F-CR7K].

[6] Patrick Coffee, *'Deepfakes' of Celebrities Have Begun Appearing in Ads, With or Without Their Permission*, THE WALL STREET JOURNAL (Oct. 25, 2022), https://www.wsj.com/articles/deepfakes-of-celebrities-have-begun-appearing-in-ads-with-or-without-their-permission-11666692003 [https://perma.cc/CZ73-XJPE].

[7] Rana Ayyub, *I Was The Victim Of A Deepfake Porn Plot Intended to Silence Me*, Huffington Post (Nov. 21, 2018), https://www.huffingtonpost.co.uk/entry/deepfake-porn_uk_5bf2c126e4b0f32bd58ba316 [https://perma.cc/K5FZ-DRM3].

[8] While not technically a deepfake, as the manipulated video did not use deepfake technology but rather different media manipulation techniques, the harms are clearly similar and relevant. *See Pelosi videos manipulated to make her appear drunk are being shared on social media*, WASH. POST (May 23, 2019), https://www.washingtonpost.com/video/politics/pelosi-videos-manipulated-to-make-her-appear-drunk-are-being-shared-on-social-media/2019/05/23/92108d20-9d32-4ba0-95bf-c37b9510e6ff_video.html [https://perma.cc/3UUD-G4K4].

to surrender.[9] While these were quickly discredited, the use of such technology in a political or conflict situation can be deeply unsettling.[10] More importantly, such uses of deepfake technology create what Danielle Citron and Robert Chesney call the Liar's Dividend, where the proliferation of deepfakes and other false information makes it "easier for liars to deny the truth."[11] The erosion of trust in society and political institutions is alarming.

There are beneficial uses of deepfake technology as well. For example, deepfakes have been used in education about the Holocaust, where the technology has enabled individuals to participate in simulated conversations with deceased Holocaust survivors.[12] Museums have started to use deepfakes to encourage more engagement with their exhibitions.[13] In the entertainment industry, the possibility of using deepfakes to improve special effects has garnered a lot of attention; in fact, the company behind Star Wars hired a YouTube deepfake artist whose edited video of a scene in "The Mandalorian" was considered better than the original.[14] Beyond art and media, the technology behind deepfakes also has crucial value in the field of medicine, where the ability to generate fake medical scans can improve the ability of doctors and scientists to conduct better diagnoses.[15] Politicians have even used deepfakes to enhance their own image: South Korean presidential candidate (now president) Yoon Suk-yeol used deepfake technology to create an AI version of himself, called "AI Yoon," that portrayed a softer public image in an attempt to win over younger voters.[16] Human Yoon was perceived

---

[9] Tom Simonite, *A Zelensky Deepfake Was Quickly Defeated. The Next One Might Not Be,* WIRED (Mar. 17, 2022), https://www.wired.com/story/zelensky-deepfake-facebook-twitter-playbook/ [https://perma.cc/2QFX-26TA].

[10] Robert Chesney, Danielle Citron & Hany Farid, *All's Clear for Deepfakes: Think Again*, LAWFARE (May 11, 2020), https://www.lawfareblog.com/alls-clear-deepfakes-think-again [https://perma.cc/NSV7-R4QX].

[11] Citron & Chesney, *supra* note 2.

[12] *Artificial intelligence project lets Holocaust survivors share their stories forever,* CBS NEWS (Apr. 3, 2020), https://www.cbsnews.com/news/artificial-intelligence-holocaust-remembrance-60-minutes-2020-04-03/ [https://perma.cc/A89V-WUKD].

[13] Dami Lee, *Deepfake Salvador Dali takes selfies with museum visitors,* VERGE (May 10, 2019), https://www.theverge.com/2019/5/10/18540953/salvador-dali-lives-deepfake-museum [https://perma.cc/Q29Q-KYDK].

[14] *Shamook: Star Wars effects company ILM hired Mandalorian deepfaker,* BBC NEWS (Jul. 28, 2021), https://www.bbc.com/news/entertainment-arts-57996094 [https://perma.cc/8V9S-XNHE].

[15] Jackie Snow, *Deepfakes for good: Why researchers are using AI to fake health data,* FAST CO. (Sept. 24, 2018), https://www.fastcompany.com/90240746/deepfakes-for-good-why-researchers-are-using-ai-for-synthetic-health-data [https://perma.cc/LB8P-UAFP].

[16] Timothy W. Martin & Dasl Yoon, *These Campaigns Hope 'Deepfake' Candidates Help Get Out the Vote,* WALL ST. J. (Mar. 8, 2022), https://www.wsj.com/articles/these-campaigns-hope-deepfake-candidates-help-get-out-the-vote-11646756345 [https://perma.cc/3NQ4-DRQH].

as being too stern and having trouble connecting with the electorate, while AI Yoon arguably boosted his popularity by being more likeable.[17]

These deeply contrasting examples highlight the tensions inherent in the use and development of deepfake technology and the difficulties in determining how strictly to regulate it. Nonetheless, given the significant interest in and the rapid improvements in quality and accessibility[18] of this technology in a variety of sectors, there is agreement across the United States, the European Union, and China that regulation is needed to manage the continued development of deepfakes. What form that regulation should take is still a matter of ambiguity.

Existing research on deepfake regulations has been limited, in part due to the recency of the proposed and implemented legislations at issue and the novelty of the technology itself.[19] At the same time, the United States, the European Union, and China are also all grappling with important related issues that will be impacted by deepfake technology, like the interaction of free speech and fake news, the amplification of misinformation during elections, and the need for data protection laws. This paper will compare and contrast regulations for deepfakes across each of these three relevant jurisdictions. In so doing, this paper will provide an early analysis of where deepfake regulations may converge, where they may diverge, and to evaluate broader philosophical differences in approach as well as opportunities for cooperation between regulators around the world. Such regulations, though generally meant to be enforceable within the territory they are implemented, tend to have global impacts, making analysis of their interactions important.

Part I of this paper will provide a deep-dive review of each of the three regulatory regimes for deepfakes and the contexts found in the United States, the European Union, and China. Part II will more closely compare and contrast the three approaches through a number of different organizing lenses. Part III will propose a normative framework for assessing the impacts of each jurisdiction's deepfake regulations and will provide suggestions on how each governmental body can improve their approach to deepfakes through understanding the similarities and differences of their approach to others'. The paper concludes with suggestions on areas for future research.

---

[17] *See id.*

[18] Jared Schroeder, *Free Expression Rationales and the Problem of Deepfakes Within the E.U. and U.S. Legal Systems* (Jan. 7, 2020), https://ssrn.com/abstract=3503617 [https://perma.cc/S5AE-W6WV].

[19] Though there have been academic analyses on the benefits and harms of the technology and acknowledgements of the difficulties in regulating it within existing laws; *see* Citron & Chesney, *supra* note 2.

I. CLARIFYING EXISTING REGULATORY PROPOSALS FOR DEEPFAKES

Starting at the turn of the 2020s, within the span of just a couple of years, a series of laws have been proposed to regulate deepfakes in the United States, the European Union, and China. Responding to concerns that deepfake videos (and audio) can deceive and manipulate,[20] there was a willingness to move quickly to limit potentially significant harms. In many ways, the resulting approaches taken by each of the three jurisdictions are emblematic of the broader philosophical and legal traditions held by each system. The approach in the United States has been led by individual states with respect to targeted uses; the approach in the European Union has been part of the larger framework for analyzing AI risks in general; and the approach in China has tended to anchor on transparency of creators and being in alignment with societal values.

A. The United States' Approach

In the United States, no federal law on deepfakes (or on AI or on data privacy) has passed or even seems likely to pass. This has left a vacuum for states to fill; California has led the charge, passing some of the first deepfake-focused laws in the country in 2019. California's two laws are simple and focus on specific applications of deepfake technology: AB730 is directed at deepfakes that can influence political campaigns, and AB602 is directed at deepfakes in pornography.[21] AB730, set to expire on January 1st, 2023 (unless renewed), prohibits the use of deepfakes within 60 days of an election and allows the candidate targeted by the deepfake to seek injunctive or other equitable relief as well as damages.[22] AB602 creates a private right of action against someone who intentionally distributes photo and video deepfakes that are of an intimate or sexual nature.[23] Other states are following suit; Texas also passed a law in 2019, similar to California's AB730, that prevents the

[20] Citron & Chesney, *supra* note 2, found that "[g]rowing sophistication of the GAN approach is sure to lead to the production of increasingly convincing and nearly impossible to debunk deepfakes."
[21] K.C. Halm et al., *Two New California Laws Tackle Deepfake Videos in Politics and Porn*, Davis Wright Tremain LLP (Oct. 14, 2019), https://www.dwt.com/insights/2019/10/california-deepfakes-law [https://perma.cc/3F7E-RZNT].
[22] Assemb. B. 730, 2019–2020 Reg. Sess. (Cal. 2019), https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201920200AB730 [https://perma.cc/ZDE3-L5XF].
[23] Assemb. B. 602, 2019–2020 Reg. Sess. (Cal. 2019), https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201920200AB602. [https://perma.cc/7HC5-7PZ2].

distribution of political deepfakes within 30 days of an election.[24] Virginia passed a law in 2019 that criminalized the distribution of pornographic deepfakes if they are "indicated to coerce, harass or intimidate a person" (in an attempt to prevent what is colloquially known as "revenge porn").[25] New York, in 2020, continued the trend of preventing pornographic deepfakes by creating a private right of action in such situations, along with a post-mortem right to protect an artist's likeness from commercial exploitation for 40 years after death.[26] It is likely that other states may follow.[27]

While there are no federal laws on regulating deepfakes, there have been attempts to do so through proposed bills in both the House and the Senate. Senator Rob Portman of Ohio introduced a bill to establish a National Deepfake Provenance Task Force in 2021, and Representative Yvette Clarke of New York proposed the Deep Fakes Accountability Act of 2019 to establish a transparency requirement of watermarks on deepfakes and criminal penalties for violations.[28] Neither of these bills have made it out of their respective committees. Instead, federal measures that have successfully passed have aimed at directing agencies to collect better information in advance of law's creation. The annual US National Defense Authorization Act for 2020 and 2021 both set aside funding for the Department of Homeland Security to research and produce reports on deepfakes.[29] Relatedly, in December 2020, Congress passed the Identifying Outputs of Generative Adversarial Networks Act which requires the National Science Foundation and the National Institute

---

[24] Texas SB 751, https://capitol.texas.gov/tlodocs/86R/billtext/html/SB00751S.htm [https://perma.cc/4T59-VNMX].

[25] Virginia House Bill No. 2678, https://lis.virginia.gov/cgi-bin/legp604.exe?191+ful+HB2678S1&191+ful+HB2678S1 [https://perma.cc/4CAG-F3GC].

[26] New York Senate Bill S5959D, https://www.nysenate.gov/legislation/bills/2019/s5959 [https://perma.cc/C93U-GR9G].

[27] *See e.g.,* Sarah Coble, *Florida Considers Deepfake Ban*, INFOSECURITY MAGAZINE (Jan. 27, 2022), https://www.infosecurity-magazine.com/news/florida-considers-deepfake-ban/ [https://perma.cc/9UK3-F4Y4].

[28] Deepfake Task Force Act, S.2559, 117th Cong. (2021), https://www.congress.gov/bill/117th-congress/senate-bill/2559/; DEEP FAKES Accountability Act, H.R.3230, 116th Cong. (2019), https://www.congress.gov/bill/116th-congress/house-bill/3230.

[29] The 2020 version was narrowly focused on national security, while the 2021 version was broader. Kelley M Sayler & Laurie A. Harris, *Deep Fakes and National Security*, CONGRESSIONAL RESEARCH SERVICE (Jun. 8, 2021), https://crsreports.congress.gov/product/pdf/IF/IF11333 [https://perma.cc/W3PX-T7W9]; *see* Jason Chipman et al., *First Federal Legislation on Deepfakes Signed Into Law*, JD SUPRA (Dec. 24, 2019), https://www.jdsupra.com/legalnews/first-federal-legislation-on-deepfakes-42346/ [https://perma.cc/3NSN-AR4S]; Matthew F. Ferraro, *Congress's deepening interest in deepfakes*, THE HILL (Dec. 29, 2020), https://thehill.com/opinion/cybersecurity/531911-congresss-deepening-interest-in-deepfakes [https://perma.cc/236N-CCRL].

of Standards and Technology to study deepfakes and other innovations that leverage this technique.[30]

The set of laws at the states level is illustrative of the United States' approach: target individual sectors and specific use cases of deepfake technology below the federal level, in elections and pornography specifically. Meanwhile, the passage of broader deepfake legislation is likely to be significantly impeded by First Amendment jurisprudence. In fact, state laws on deepfakes in elections were controversial because of the concern that they are incompatible with the right to free speech.[31]

Though there continues to be debate on the First Amendment's application to deepfakes, there is a growing sense among legal scholars that deepfakes are a form of First Amendment expression.[32] This is driven by the critical 2012 Supreme Court decision *United States v. Alvarez*, which established that false statements can receive First Amendment free speech protection.[33] As such, deepfakes, even when used as intentional falsehoods, are likely to be protected in some form under the right of free speech. However, just because it is First Amendment expression does not mean it is always protected speech since, as the *Alvarez* case itself went on to indicate, lies can be punished when the falsity leads to serious legally-cognizable harms.[34] Therefore, if there is clear harm and a prohibition is specific to resolving that harm, then there is a stronger argument to be made for limiting deepfakes under a strict scrutiny standard of review.[35] As such, it becomes

---

[30] *Id.*

[31] Matthew Feeney, *Deepfake Laws Risk Creating More Problems Than They Solve*, REGULATORY TRANSPARENCY PROJECT OF THE FEDERALIST SOCIETY (Mar. 1, 2021), https://regproject.org/paper/deepfake-laws-risk-creating-more-problems-than-they-solve/ [https://perma.cc/6HC2-8RFX].

[32] *See generally* Nina I. Brown, *Deepfakes and the Weaponization of Disinformation*, 23 VA. J.L. & TECH. 1 (2020) [https://perma.cc/VZQ6-HBZE]; Marc Jonathan Blitz, *Deepfakes and Other Non-Testimonial Falsehoods: When is Belief Manipulation (Not) First Amendment Speech?*, 23 YALE J.L. & TECH. 160 (2020) [https://perma.cc/DU7T-86KM]; Cass R. Sunstein, *Falsehoods and the First Amendment*, 33 HARV. J.L. & TECH. 388 [https://perma.cc/G8M9-XAMC];Citron & Chesney, *supra* note 2.

[33] In that case, the criminal defendant, Xavier Alvarez, lied about receiving a Congressional Medal of Honor for bravery in battle and was prosecuted for false representation under Congress' Stolen Valor Act. It was this Stolen Valor Act that was deemed unconstitutional by the Supreme Court. *See* United States v. Alvarez, 567 U.S. 709, 723-4 (2012).

[34] *See* Blitz, *supra* note 32, at 171 (2020) ("What makes deepfakes a challenge for First Amendment analysis is that they straddle the line between the realm that the First Amendment reserves for authorship and the informational realm external to speakers' words (which they do not have a First Amendment right to shape)"); *See* Alvarez, *supra* note 33 (plurality opinion).

[35] There is an interesting debate regarding how to know what harms are legally cognizable in a fast-moving technology-enabled environment. *See id.* (analyzing Justice Breyer's opinion versus Justice Kennedy's opinion in *United States v. Alvarez*).

clear why the focus of existing deepfake regulations has been on election interference and revenge porn—these are targeted and egregious risks and the prohibitions have been narrowly tailored.

Another unique element of American jurisprudence is the extent to which platforms—the main medium through which deepfakes circulate—are generally shielded from liability for the content found on their sites and apps. Section 230 ensures that platforms are not liable for hosting harmful material that they did not create.[36] Because of this, state-level regulations are also restricted in their impacts as they cannot hold platforms liable for the deepfakes found on them. This, as will be seen in the following sections, places the United States at odds with the European Union and China, where regulators are seeking to make platforms responsible in some form. The reason is simple: it is more efficient to go after the platforms that host deepfakes than to go after hundreds of individual and frequently anonymous creators.[37] Some commentators have argued that, without the ability to impose requirements on platforms, any regulation of deepfakes is unlikely to succeed.[38] As a result, the ruling from the upcoming *Gonzalez v. Google* case in front of the Supreme Court should be watched closely for the future ability to regulate deepfakes on platforms, as the question before the court in that case will be whether immunity under Section 230 of the Communications Decency Act exists when platforms' algorithms target users with someone else's content.

B. The European Union's Approach

While the European Union is known for moving quickly to establish laws that protect consumers and data from innovative emerging technologies, there have been relatively limited standalone discussions about deepfake laws at the union level. This is because the European Union has been very focused on developing overarching frameworks and the governance of artificial intelligence is no exception.[39] This is not to say that other regulations do not have relevance for the governance of deepfakes. In fact, a European Union policy paper noted nine regulatory frameworks that all have implications for how deepfakes can be used and created.[40] However, deepfakes are only

[36] Citron & Chesney, *supra* note 2.
[37] Greg Parker, *Legislating Deepfakes: The Internet's Newest Stalemate Between Lawmakers and Tech Companies*, COLUMBIA BUS. L. REV. (2019), https://journals.library.columbia.edu/index.php/CBLR/announcement/view/236 [https://perma.cc/B9FQ-KXEH].
[38] Citron & Chesney, *supra* note 2.
[39] For example, the General Data Protection Regulations (GDPR), the Digital Services Act (DSA), the Digital Markets Act (DMA), etc.
[40] *See* Eur. Parliamentary Rsch. Serv., *supra* note 5, at VI.

directly legally acknowledged in the European Union's recent Artificial Intelligence Act, or AI Regulations,[41] as well as a couple of parliamentary action plans against disinformation and resolutions on education.

The AI Regulations, proposed in April 2021, established a holistic and unified risk-based approach to regulating all artificial intelligence practices.[42] The AI Regulations looked at the lifecycle of how AI systems are designed, built, and run,[43] and distinguished between categories of AI by the risks posed. Specifically, there are certain AI practices that are prohibited outright and there are high-risk AI systems that are subject to a compliance regime with detailed requirements. Interestingly, deepfake technology is not a prohibited AI practice, and it is not clear whether deepfakes fall in the high-risk AI category. Instead, deepfakes are explicitly called out in Title IV (Article 52) as posing manipulation risks (along with chatbots and emotion recognition systems) and, therefore, are subject to certain transparency requirements, meaning it must be disclosed if content has been manipulated or artificially generated.[44] There is, however, no discussion of how the disclosure should be provided, nor are there any clear penalties for non-compliance.[45]

There are two nuances in the AI Regulations that highlight a balancing of different rights. The first is an exception to the labelling requirement when "the use is authorized by law to detect, prevent, investigate and prosecute criminal offences or [the use] is necessary for the exercise of the right to freedom of expression and the right to freedom of the arts and sciences."[46] While the focus on "the right to freedom of expression and the right to freedom of the arts and sciences" seems to place a high bar on restricting deepfakes, the European Union has generally viewed information as a "public good that must be cared for by lawmakers and judges alike,"[47] which also implies a strong focus on truthful information. Additionally, the European Union legal system, while valuing free expression, does seek to balance it with other

---

[41] *See* Mark MacCarthy & Kenneth Propp, *Machines Learn that Brussels Writes the Rules: The EU's New AI Regulation,* LAWFARE (Apr. 28, 2021, 10:51 AM), https://www.lawfareblog.com/machines-learn-brussels-writes-rules-eus-new-ai-regulation [https://perma.cc/7SY2-2VG3].

[42] Eur. Comm'n, *Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts*, COM (2021) 206 final (Apr. 21, 2021), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELLAR%3Ae0649735-a372-11eb-9585-01aa75ed71a1, [https://perma.cc/ZHR9-5R3Y].

[43] DLA PIPER, *EU AI Regulation Handbook: The Future Regulation of Technology* (2021).

[44] *See* Eur. Comm'n, *supra* note 42("[f]or some specific AI systems, only minimum transparency obligations are proposed, in particular when chatbots or 'deep fakes' are used.").

[45] *See* EUR. PARLIAMENTARY RSCH. SERV., *supra* note 5, at 38.

[46] DLA Piper, *supra* note 43, at 25.

[47] Schroeder, *supra* note 18.

human rights, such as privacy, making the free speech argument against deepfake regulations less of a barrier in the European Union compared to the United States. It also indicates that the European Union is willing to tolerate some censorship of deepfake speech in order to protect other rights. The second nuance is the categorization of the uses of deepfake technology as high-risk AI systems in the specific situation of being "used by law enforcement authorities … to detect 'deepfakes'" in order to protect the rights and freedoms of individuals.[48] This is a recognition that there is some value in the creation of deepfakes such that the use of deepfake detection technology by law enforcement has to be done thoughtfully.[49]

Outside of the AI Regulations, the European Parliament has discussed deepfakes in several resolutions. Specifically, in a resolution adopted in May 2021, the European Parliament emphasized the importance of raising awareness and improving digital literacy in order to enable society to detect and label deepfakes more effectively.[50] The resolutions suggest that any regulation of deepfakes cannot stop at limiting the use of the technology or the creation and distribution of the content, but must also strengthen the ability of individuals to be aware of the risks from and be better able to recognize deepfakes.[51] Ultimately, manipulation by synthetic media, which will continue to improve, cannot be diminished without working with the targets of deepfakes and developing strategies for individuals to recognize deepfakes.

C. China's Approach

Concerns with AI-generated media in China began with the availability and heightened popularity of apps that allow users to create their own deepfakes.[52] In 2019, an app called ZAO gained popularity for enabling users to "swap faces" but quickly ran into controversy over its data collection

[48] *See* Eur. Comm'n, *supra* note 42.
[49] Europol Innovation Lab, *Facing Reality? Law Enforcement and the Challenge of Deepfakes*, EUROPEAN UNION AGENCY FOR LAW ENFORCEMENT COOPERATION (2022), https://www.europol.europa.eu/publications-events/publications/facing-reality-law-enforcement-and-challenge-of-deepfakes [perma.cc/LX45-D2NV].
[50] European Parliament, *Resolution of 19 May 2021 on artificial intelligence in education, culture and the audiovisual sector*, P9_T0238, (May 19, 2021) [https://perma.cc/2WR3-6SVL].
[51] *Id.*
[52] This includes both standalone apps and related functionalities within preexisting popular apps. *See* Zehi Yang, *Chinese Deepfakes Are Going Viral, and Beijing Is Freaking Out*, PROTOCOL (Mar. 19, 2021), https://www.protocol.com/china/chinese-deepfakes-regulators-alibaba-tencent [perma.cc/2UJ2-PCV3].

policies.[53] While ZAO has since altered its privacy agreements dramatically, the societal backlash drove the Chinese authorities to their first official attempt to regulate deepfakes—and to even consider banning it completely.[54] The Cyberspace Administration of China published multiple articles, all within three months of ZAO's launch, that discussed the need to develop AI regulations and govern AI development. This ultimately led to the publication of the "Regulations on the Administration of Networked Audiovisual Information Services" in November 2019 (with an enforcement date of January 1, 2020).[55]

The 2019 regulations created new rules and responsibilities for both the providers of "audio and video information services" as well as the users of such services. Many media outlets noted that the rules made it a criminal offense to publish deepfakes without clearly labeling them as such and that they banned the use of deep learning and virtual reality to produce fake news.[56] Unlike in the United States, where platforms are protected from liability by Section 230, there is a heavy focus on the role of platforms to police content, including conducting security assessments, developing technology to detect deepfakes, proactively tagging deepfakes, and preventing circulation of and reporting illegal deepfakes.[57] In other words, the 2019 regulations clarified that the "network audio and video information services providers" are responsible for managing the information content of their platforms; meanwhile, both the "service providers" and the individual users of deepfake-

---

[53] Gabriele de Seta, *Huanlian, or changing faces: Deepfakes on Chinese digital media platforms*, 27 CONVERGENCE: THE INTERNATIONAL JOURNAL OF RESEARCH INTO NEW MEDIA TECHNOLOGIES 935, 941 (2021).

[54] *China seeks to root out fake news and deepfakes with new online content rules*, REUTERS (Nov. 29, 2019), https://www.reuters.com/article/us-china-technology/china-seeks-to-root-out-fake-news-and-deepfakes-with-new-online-content-rules-idUSKBN1Y30VU [perma.cc/Z656-JU7F].

[55] *Regulations on the Administration of Networked Audiovisual Information Services*, CYBERSPACE ADMIN. OF CHINA (Nov.18, 2019), http://www.cac.gov.cn/2019-11/29/c_1576561820967678.htm [perma.cc/E2DQ-ZHCQ]. This document was jointly formulated by the Cyberspace Administration of China, the Chinese Ministry of Culture and Tourism, and the National Radio and Television Administration of China.

[56] Reuters, *supra* note 54; Meng Jing, *China issues new rules to clamp down on deepfake technologies used to create and broadcast fake news*, SOUTH CHINA MORNING POST (Nov. 29, 2019), https://www.scmp.com/tech/apps-social/article/3039978/china-issues-new-rules-clamp-down-deepfake-technologies-used, [perma.cc/6WAK-9SXU].

[57] Specifically, Article 10 of the regulations requires security assessments for content based on new technologies and applications such as deep learning and VR; Article 11 requires prominent identification of deepfakes and bans the production and dissemination of fake news created by "deep learning and virtual reality" technologies; and Article 12 requires stronger information management by service providers of deepfakes, including the detection and reporting of illegal deepfakes. *See* CYBERSPACE ADMIN. OF CHINA, *supra* note 55.

creating services could be held liable for prosecution.[58] When introducing the regulations, the Cyberspace Administration of China emphasized that the use of new technologies, such as deepfakes, in online videos and audio can "disrupt social order and violate people's interests, creating political risks and bringing a negative impact to national security and social stability."[59]

Deepfake videos have continued to be popular in China, with Bilibili being one of the most utilized platforms on which these videos are shared.[60] Generally, the deepfake videos in China have tended toward changing actor and celebrity faces for entertainment rather than political or news purposes.[61] Then in January 2022, the Cyberspace Administration of China released another set of proposed rules—the "Regulations on Deep Synthesis Management of Internet Informaiton Services"—or comments and public consultation;[62] ten months later, the final official regulations were published with an enforcement date of January 10, 2023.[63]

These 2022 regulations more directly targeted deepfakes because they demand specific responsibilities for the management of "deep synthesis" technologies and services by "internet information services" providers (a category that is broader than and encompasses "audio and visual information services" providers). However, though deepfakes are the most common outputs of such technologies, the definition of "deep synthesis technologies" is quite a bit broader than that of deepfakes; they refer to technologies that create "text, images, audio, video, virtual scenes and other information using deep learning, virtual reality and other synthetic-generating algorithms" and, therefore, includes virtual and/or immersive environments, chatbots, as well

---

[58] Nick Statt, *China makes it a criminal offense to publish deepfakes or fake news without disclosure*, THE VERGE (Nov. 29, 2019), https://www.theverge.com/2019/11/29/20988363/china-deepfakes-ban-internet-rules-fake-news-disclosure-virtual-reality [perma.cc/VJK3-R8R8].

[59] Quoted in Jing, *supra* note 56.

[60] de Seta, *supra* note 53.

[61] *Id.* (including ones of controversial figures like Donald Trump).

[62] *Regulations on deep synthesis management of internet information services (Draft for Comments)*, CYBERSPACE ADMIN. OF CHINA (Jan. 28, 2022), http://www.cac.gov.cn/2022-01/28/c_1644970458520968.htm [https://perma.cc/L7FR-3LVK]; Josh Ye, *China targets deepfakes in proposed regulation governing deep learning AI technologies*, SOUTH CHINA MORNING POST (Jan. 29, 2022) https://www.scmp.com/tech/policy/article/3165244/china-targets-deepfakes-proposed-regulation-governing-deep-learning-ai [perma.cc/MGR5-6CNX].

[63] *Regulations on deep synthesis management of internet information services*, CYBERSPACE ADMIN. OF CHINA (Nov. 25, 2022), http://www.cac.gov.cn/2022-12/11/c_1672221949354811.htm [https://perma.cc/4XWS-5TR3]. This was jointly published by the Cyberspace Administration of China, the Chinese Ministry of Industry and Information Technology, and the Public Security Ministry of China.

as deepfakes.[64] Written in this manner, the law seeks to regulate the ways in which the underlying technologies are used rather than the outputs (deepfakes or otherwise) of the technologies. The new regulations on deep synthesis management echo many of the requirements of the 2019 rules on audio and video information services, including: a heavy focus on the role of platforms, the need to conduct real-name identity verification of all users, the tagging of deepfakes, the possibility of criminal prosecution in addition to civil penalties, and the focus on social morality and correct political direction. The 2022 regulations do also add additional points of emphasis: there is a focus on strengthening training data management as well as on technical management,[65] and, most interestingly, there is a requirement that platforms must remind users that notification need to be given and consent obtained prior to using other people's facial and vocal likeliness in deepfakes.[66]

In the Chinese context, these deepfake regulations were among (and references) multiple sets of regulations on a variety of emerging technologies, algorithms, and consumer data privacy issues. For example, a few weeks prior to first proposing the 2022 regulations, the Cyberspace Administration of China also issued regulations on controlling algorithms used to make recommendations on platforms and apps, including transparency requirements and optimization requirements for datasets.[67] As such, the deepfake laws should be viewed as part of a much broader push by Chinese authorities to manage the digital environment.[68]

---

[64] Interestingly, the inclusion of virtual reality in the definition for "deep synthesis" can indicate a concern about forthcoming technologies that build upon deepfake technologies, such as those that will be used to create a "metaverse". *Regulating tech use to curb 'deepfake' risks*, CHINA DAILY (Dec 14, 2022), https://global.chinadaily.com.cn/a/202212/14/WS63990f95a31057c47eba440e.html [https://perma.cc/B7SZ-ZT8U]; *Responding to Journalists' FAQs on Regulations on deep synthesis management of internet information services,* CYBERSPACE ADMIN. OF CHINA (Dec. 11, 2022), http://www.cac.gov.cn/2022-12/11/c_1672221949570926.htm [https://perma.cc/R8QT-ERJR].

[65] Chapter III of the regulations discusses data and technical management, *see* CYBERSPACE ADMIN. OF CHINA *supra* note 64.

[66] Ye, *supra* note 62; Ben Jiang, *China's internet censors target deepfake tech to curb online disinformation*, SOUTH CHINA MORNING POST (Dec. 12, 2022), https://www.scmp.com/tech/policy/article/3203000/chinas-internet-censors-target-technology-behind-deepfakes-curb-online-disinformation [https://perma.cc/6XSB-EQLB].

[67] Samuel Adams, *China's draft algorithm regulations: A first for consumer privacy,* IAPP (Oct. 13, 2021), https://iapp.org/news/a/chinas-draft-algorithm-regulations-a-first-for-consumer-privacy/ [https://perma.cc/NHR7-WPWG].

[68] Jennifer Conrad & Will Knight, *China Is About to Regulate AI – and the World Is Watching*, WIRED (Feb. 22, 2022), https://www.wired.com/story/china-regulate-ai-world-watching/ [https://perma.cc/9ZCX-UDDT].

II. ARTICULATING SIMILARITIES AND DIFFERENCES ACROSS THE THREE JURISDICTIONS

In facing the challenges of AI-generated media, the United States, the European Union, and China have taken different approaches. These approaches vary in the rules proposed, the actors regulated, and the consequences imposed. None have completely banned the technology, and all acknowledge the value of transparently marking deepfakes. Through a closer analysis of the similarities and differences, this part of the paper will describe three distinct, but not mutually exclusive, methods for categorizing deepfake regulations. In so doing, Part III will then provide a view into opportunities for collaboration between the differing regulatory regimes through an outcomes-focused framework.

A. Regulating Specific Stages Along the Deepfake Lifecycle

One way to categorize deepfake regulations is by focusing on the deepfake lifecycle, from creation through distribution and consumption. As described in the European Union policy paper on "Tackling deepfakes in European policy," there are five distinct areas, aligned to the stages of the deepfake lifecycle, where deepfakes could be regulated: (1) the technology itself; (2) the creation of a piece of deepfake content; (3) the circulation of that content; (4) the target (if any) of that content, and; (5) the audience who views the content.[69] Essentially, the question being asked here is where in the deepfake lifecycle should policymakers attempt to regulate deepfakes.

Viewed from this organizing principle, there are some clear distinctions in emphasis across jurisdictions. Specifically, both the European Union and China tend to focus on the earlier stages of the lifecycle (the technology, the creation, and the circulation pieces), while the United States tends to focus on the later stages (the target and audience stages). For the European Union, the AI Regulations put an emphasis on tagging deepfakes by the creators and circulators since the technology is categorized as having manipulation risk. For China, the focus on the underlying technology, the requirements for creators to use real names and ID numbers on platforms that provide deepfake technology, and the demand for platforms to oversee and tag deepfakes are clearly regulating the two early stages of the deepfake lifecycle; similarly, the requirement that platforms are accountable for tagging

[69] A European Parliament research provides five phases of the deepfake lifecycle: technology, creation, circulation, target, audience. *See* EURO. PARLIAMENTARY RSCH. SERV., supra *note* 5, at 58 (July 2021), https://www.europarl.europa.eu/RegData/etudes/STUD/2021/690039/EPRS_STU(2021)690039_EN.pdf [https://perma.cc/QE78-J2MA].

deepfakes and for limiting reposts of deepfake news target the circulation stage. For the United States, while some of the prohibition on deepfakes in elections and pornography appear to be focused on the earlier creation stage, the underlying concern is about giving rights of action to the target and audience of the deepfakes which indicates that the United States' laws are actually motivated by concerns toward the later stages of the lifecycle.

This analysis is not to say that the three jurisdictions do not also each consider the other stages of the lifecycle. Rather, recognizing which stages of the deepfake lifecycle appear most concerning can highlight differences in "who" is held accountable and responsible. There are five distinct groups who are impacted by deepfake laws: (1) the providers of the deepfake technology, (2) the platforms for distributing deepfakes, (3) the individual creators of deepfakes, (4) the people whose images are falsified or who are harmed/manipulated by the deepfakes, and (5) the public that views the deepfakes. As stated in a European Union policy paper:

> "Typically, different actors are involved in the lifecycle of a deepfake. These actors might have competing rights and obligations. […] This leads to the conclusion that policy-makers, when aiming to mitigate the potential negative impacts of deepfakes, should take different dimensions of the deepfake lifecycle into account."[70]

For the European Union and China, where deepfake laws have tended to focus on the early stages, platforms and individual creators are frequently the target of regulations.[71] In the case of the European Union, the resolutions on educating the public to recognize deepfakes would focus on the last stage of the deepfake lifecycle, however there is no law explicitly implementing this idea as yet. Meanwhile, in the United States, because the regulatory focus is on protecting the individuals who receive or whose images are used in deepfakes, the currently-existing laws tend to work by giving individuals the

[70] *See* EUR. PARLIAMENTARY RSCH. SERV., *supra* note 5, at VI (providing additional examples that "perpetrators often act anonymously, making it harder to hold them accountable. It seems that platforms could play a pivotal role in helping the victim to identify the perpetrator. Moreover, technology providers also have responsibilities in safeguarding positive and legal use of their technologies").

[71] Particularly in China, the focus is on impacting the behaviors of providers of "internet information services" and providers of "network audio and visual information services." The two regulations discussed in this paper do contain articles that require the existence of methods for the public to make complaints; hence, there is some acknowledgement of possible redress for the individuals who receive deepfakes or whose images are used in deepfakes, but that is not the main objective of either regulation.

responsibility and the burden of bringing causes of action and suing for injunctions after the distribution of a deepfake.

B. Regulating by Sector or Risk Assessment

A second organizing principle is whether a deepfake law should regulate by sector (i.e., use case) or by level of risk (i.e., via a risk assessment). The former would create distinct rules for specific deepfake uses, such as for electioneering or fake news, whereas the latter would look more at the potential risks of an application of deepfakes regardless of sector, industry, or use case. The United States, by targeting elections and pornography, clearly regulates by sector or use case (though there is also an implicit understanding that the selected sectors generally lead to higher risk).[72] This approach is rather blunt, as it seeks to prohibit specific deepfake uses regardless of whether the content is positive or negative. Consider the example of AI Yoon at the beginning of this paper: Even in electoral situations, it is possible to use deepfakes in a positive way if it is clearly noted to be a deepfake; yet a similar use would now be illegal under Californian and Texan law in the United States when close to an election.

The European Union proposes to regulate explicitly from a risk assessment framework. In fact, though deepfakes are part of a unique "manipulation risk" category in the AI Regulations, deepfake uses also need to go through a risk assessment analysis. It is possible for a deepfake use to be subject both to Title IV Article 52 transparency obligations, which are exclusive to AI practices that pose manipulation risks, and to Title III Articles 8-15 if that specific deepfake practice is determined to be "high risk."[73]

The Chinese case seems to have evolved slightly between the publication of the two deepfake-relevant laws in 2019 and 2022. The 2019 law was perceived as a ban on fake news, a specific use case of deepfakes, and aimed at audio and visual elements on the internet.[74] In its aftermath, as deepfakes continued to be popular in entertainment and pop culture, the Cyberspace Administration of China decided to focus broadly on the underlying technologies that enable deepfakes so as not to assume the form in which future uses of such technologies could take. The 2022 laws, as a result, applies to all deepfakes and related outputs that use "deep synthesis" technologies rather than any specific use case of deepfakes. In fact, the 2022 regulations affirm that any new application of "deep synthesis" technologies must go through rigorous review. In this sense, China is mostly regulating

[72] Parkin, *supra* note 3.
[73] DLA Piper, *supra* note 43.
[74] *See* Jing, *supra* note 56.

from a risk analysis approach, like the European Union, though with some focus on the specific harms from fake news.

C. Regulating Individually or as Part of a Holistic AI Strategy

The third way to organize approaches to deepfake regulations is by whether the authorities have regulations specifically targeting deepfakes, or whether it is part of a broader, holistic AI framework. Given how quickly technologies change, there is much to be said about defining a high-level philosophy of how to manage and govern all new technologies, including deepfakes. On the other hand, there are unique harms that result from this technology, and a targeted regulation would enable a more nuanced and detailed response.[75]

In this regard, the United States is tackling deepfakes from an individual technology perspective. The interest has been on the details of the deepfake techniques and where and when they are used. On the opposite side, the European Union explicitly includes deepfake as just another technology under its broad AI Regulations. In China, the existence of the new law on "deep synthesis technologies" indicates the decision to regulate deepfakes and related technologies individually and in a targeted manner due to concerns about the rapid development of such technologies;[76] however, the broader legal context in China reveals that this law should be viewed as part of and connected to a set of inter-related laws focused on managing AI and the digital ecosystem.[77]

One benefit of regulating as part of a holistic AI strategy is the ability to find common harms and common solutions. For example, several European Union proposals have focused on the need for broader education campaigns to teach citizens how to recognize false information online, whether in the form of deepfakes or otherwise.[78] In the long run, such solutions may have more

---

[75] A similar distinction exists in privacy law, where the US provides "notice and choice" style of data protection generally on a sector-by-sector basis (though this may be changing with some states seeking to implement more holistic privacy laws), whereas the European Union looks at privacy more broadly and comprehensively via the GDPR. *See* Neil Richards and Woodrow Hartzog, *Why Europe's GDPR magic will never work in the US,* WIRED UK (Feb. 20, 2020), https://www.wired.co.uk/article/us-version-gdpr [https://perma.cc/84J8-AZRV].

[76] Jiang, *supra* note 66.

[77] Conrad & Knight, *supra* note 68.

[78] One of the two priority areas in the EU's Digital Education Action Plan (2021-2027) is on "enhancing digital skills and competences for the digital transformation" which includes improvements in digital literacy and the tackling of disinformation through education and training. *See* EUROPEAN UNION, DIGITAL EDUCATION ACTION PLAN (2021-2027), https://education.ec.europa.eu/focus-topics/digital-education/about/digital-education-action-plan [https://perma.cc/2ZFH-V92S].

success and longevity in limiting the negative impacts of emerging and often-changing technologies. In a similar manner, all Chinese laws on AI and emerging technologies include a reference to moral and socialist values which, albeit concerningly paternalistic, is an indication of a more holistic approach for society, rather than just protecting individuals from harm on a case-by-case basis.[79]

	United States	**European Union**	**China**
Focused on which stage(s) of the deepfake lifecycle?	Focused on later stages (impact on audience and target)	Across entire lifecycle but focused on early stages (technology and creation)	Across entire lifecycle but focused on early stages (technology, creation, and circulation)
Focused on use cases of deepfake technology or focused on analyzing the risks resulting from the technology?	Use cases	Risk analysis	Mostly risk analysis
Targeting deepfakes individually or as part of a holistic AI framework?	Individually	Holistic	Both, law targeted to deepfake technology that is part of a broader holistic AI strategy
Any enforcement mechanisms?	Varies by states – generally injunction and damages	Unclear	Varies according to relevant related laws, includes criminal prosecution
Who will be held accountable for harms?	Individual creators of specific types	Platforms and creators	Platforms and individual creators
Main (selected) regulatory requirements?	• Prohibition in very narrow situations • Private rights of action	• Tagging • Platform responsibility • Societal education campaigns	• Platform responsibility • Tagging • Creator identification

[79] Ye, *supra* note 62.

			• Criminal and civil prosecution

Fig. 1: Comparing Approaches Across Key Factors

III. LEARNING FROM EACH OTHER TO REACH OUTCOMES-BASED REGULATIONS

This paper thus far has provided observations on the current regulatory landscapes for deepfakes in the United States, the European Union, and China, and analyzed different organizing principles for those regulations. Though the contexts and the philosophies behind the regulations are different, there is a large degree of overlap in the instruments being considered to regulate deepfakes, even if the tactics ultimately selected in the relevant regulations are inconsistent. As such, there is an opportunity to uncover ways in which the different approaches may actually complement and learn from each other. But how should we think about assessing the soundness of these laws?

An obvious but frequently forgotten aspect of deepfakes, and most new technologies, is that they are not inherently good or bad. Instead, their use results in either good or bad outcomes. Consequently, we must start with the outcomes we hope to achieve with deepfake regulations and evaluate to what extent a regulation leads to that outcome. For example, if the desired outcome is to ensure that viewers of deepfakes are not tricked into believing they are authentic, then tagging is a great start–but likely insufficient. Instead, a comprehensive approach to deepfake identification will need to complement tagging–which can be done in a nondescript manner–with broader education for individuals and with effective penalties for lack of compliance.[80] Or, if the desired outcome is to prevent unfair advantage in elections through the use of deepfakes, then prohibiting them can help. However, it is unclear what timeline is appropriate and not contrived when it comes to banning deepfakes in advance of an election. Why sixty days in California versus thirty days in Texas, for example? Given how early campaigns tend to begin, are these timelines actually helpful? Such a ban would also prevent uses that are beneficial and clearly marked, such as the use of "AI Yoon" by South Korean president Yoon. Meanwhile, if the goal is to enable thoughtful innovation, then platform and creator responsibility is important but regulations that are heavy-handed and place broad or unclear limitations on who can use deepfake technology can be counterproductive.

[80] *See* Eur. Parliamentary Rsch. Serv., *supra* note 5, at 60.

Many of the tactics in the laws already discussed can work well together. For example, it is important to have both an overarching philosophy about AI as well as sector-specific rules in targeted high-risk areas. Similarly, it is crucial to have the right level of regulations at each stage of the deepfake lifecycle, rather than focusing laws on just one piece of the lifecycle. Viewed in this way, there is significant opportunity for authorities in each jurisdiction to learn from the regulations of other jurisdictions and to seek to develop a multi-layered framework that is outcome-focused–and that allows for change with a fast-innovating technology. The fact that laws are territorial but technologies are borderless is often said to be a problem.[81] But the fact that all jurisdictions are dealing with the same challenges from these technologies indicates that authorities in different jurisdictions can learn from each other to uncover their own blind spots. By clarifying the lens through which deepfake regulations can be organized, this paper aims to facilitate this process by providing a framework for authorities to evaluate where other jurisdictions' laws may complement and support their own existing deepfake laws. The organizing principles presented here do not force a selection of one or another. Rather, they highlight the importance of considering all aspects to achieve appropriate outcomes: potentially regulating against all stages of the deepfake lifecycle, regulating by sector *and* by risk assessment, and regulating by the technology individually *and* as part of a holistic AI strategy.

Across the United States, the European Union, and China, regulatory proposals have tended to highlight the legal and philosophical contexts of their jurisdiction. As these regulations start to be enforced, it behooves authorities to take stock of the impacts and consequences in other jurisdictions in addition to their own. There is much work to be done to define the precise outcomes society deems desirable when regulating deepfakes, and additional research will be needed to understand the details of which specific combinations of deepfake regulatory tactics will result in which specific desired outcomes. But it is clear that existing regulations have the potential to work together to provide a more comprehensive and multi-layered outcomes-focused approach.

CONCLUSION

The flurry of enacted and proposed deepfake regulations in the past few years has revealed a profound unease with the potential harms this emerging technology poses. The concern is consistent across the three jurisdictions discussed. Yet authorities in all three jurisdictions have avoided banning deepfake technology entirely due to recognizing its potentially

[81] Anupam Chander & Haochen Sun, *Sovereignty 2.0*, GEO. LAW FAC. PUBL'NS AND OTHER WORKS 2404, UNIV. OF HONG KONG FAC. OF LAW RSCH. PAPER No. 2021/041 (2021).

beneficial uses. In analyzing, comparing, and contrasting deepfake regulations across these jurisdictions, this paper provides three organizing principles: (1) regulating specific stages in the deepfake lifecycle, (2) regulating against sectors versus risk assessments, and (3) regulating deepfake technology on its own versus as part of a broader AI strategy. Recognizing how to organize deepfake regulatory approaches is critical to enabling authorities to learn from each other and to recognize where their blind spots might be in the journey toward a truly-sound, outcomes-based regulatory environment for deepfakes. The choices made by the United States, the European Union, and China so far have been emblematic of each system's broader philosophical and legal traditions. However, effective regulations must focus on the desired outcomes sought rather than defaulting to such traditions, and additional research will be essential for aligning tactics to outcomes. Authorities should pay attention to all possible approaches as they seek to define the right set of regulatory tactics for driving specific desirable outcomes in managing the development and application of deepfakes.