6

Chinese and Russian Cybercrime in Global Racial Orders of Intellectual Property

Anjali Vats

When President Joseph Biden retired the China Initiative,[1] an economic espionage program created in 2018 by the US Department of Justice to combat an alleged epidemic of trade secret theft carried out by those of Chinese descent, many rejoiced.[2] The government policy was derided then and now by racial justice advocates as a McCarthy style witch hunt,[3] that involved cases reminiscent of the attack on nuclear scientist Wen Ho Lee.[4] Though civil rights advocates have made clear that retiring the China Initiative is insufficient to completely upend the racist narratives routinely imposed upon people of East Asian descent,[5] some maintain that forcing prosecutors to drop cases against academics such as Anaming Hu and Gang Chen will encourage them to confront and even address their Sinophobic bias.[6]

The Trump Administration's rationale for the China Initiative, which Biden has openly criticized, stereotyped Chinese people as inherently disloyal.[7] This is the same troubling theme that prosecutors leveraged in Lee's case, now widely regarded as a Clinton Era political prosecution used to provide an alibi for trade policy that Republicans critiqued as Sinophilic.[8] As political scientist Stephen del Visco shows, the contemporary recurrence of the trope of East Asians as turncoats is not a historical accident but an intentional rhetorical strategy crafted by conservative commentators to unite the party around whiteness and capitalism.[9] Perhaps the most compelling evidence of the China Initiative's systemic bias is the case-by-case deconstruction of the indictments in the *MIT Technology Review* that revealed a prosecutorial pattern of targeting those who were #Researching-WhileAsian.[10] US officials have not yet outlined how they will restructure the China Initiative.[11] But comments by Matthew Olsen, Assistant Attorney General

for National Security, that "the department's work will not be hampered" suggests that future policy will continue to be racially problematic.[12]

The China Initiative's Sinophobia reflects American use of *intellectual property rights talk*, a term I introduce as a play on Mary Ann Glendon's notion of "rights talk," as a means of explicitly and implicitly deploying racist and sexist dog whistles to justify inequitable knowledge production, ownership, and circulation policies grounded in white and masculine theories of rights.[13] The desire to protect American intellectual property rights is so intense that it spills over into nearby areas of law—here theft of trade secrets via cyberespionage[14]—and encourages aggressive and imprecise prosecutions in the name of national security.[15] The concept of intellectual property rights talk is a useful entrée into understanding how "relational racialization," racial bias that operates *across* racial groups, operates to produce durable forms of gendered racism.[16] In this case, the China Initiative, a reflection of the white nationalist ideologies that became tools of Sinophobic populist incitement during the Trump Administration, invoked and reproduced anti-Asianness.[17] This is partly because it privileged intellectual property *rights* over intellectual property *responsibilities*, specifically about whether US demands were fair and just and what obligations might come with the US legal conceptions of trade secret infringement, especially with respect to legal issues such as cybercrime, around which there is little international consensus.[18] A wealth of literature already compellingly makes the case that imposing intellectual property standards on other nations reenacts (neo)colonial power relations, especially when done without regard for the histories and economies of those places.[19]

This chapter compares the laws imposed and punishments enforced against China with those laws imposed and punishments enforced against Russia, another nation engaged in the theft of trade secrets via cyberespionage, in order to show how (neo)colonialism emerges in international arenas, vis-à-vis disparate raced and gendered treatment in geopolitical dealings. While Chinese nationals have been historically and contemporarily singled out for acting as what I have previously described as "bad intellectual property citizens,"[20] Russian nationals have been treated with near impunity despite creating similarly alarming threats to political and economic stability.[21] Reading US engagements with these nations in relation to one another reveals a lack of racial evenhandedness in economic espionage policy that reinforces global racial and gender hierarchies of intellectual property. Greater focus on intellectual property rights responsibilities and the ethical obligations that flow from them with respect to race, gender, and nation can help to create more equitable forms of policymaking.

This chapter also complicates the binary of good intellectual property citizenship/bad intellectual property citizenship that I have previously proposed by showing that groups do not merely comply with or violate intellectual property laws. Rather, intellectual property rights talk constantly defines and redefines

"intellectual property" and "infringement" in response to real and perceived threats, frequently by employing rhetorics of race, gender, and nation to justify expansive and inequitable definitions of both. For instance, China *becomes* a worse intellectual property citizen and Russia *becomes* a better bad intellectual property citizen when Former Attorney General Jeff Sessions declares: "Perhaps this threat [from China] has been overshadowed in the press by threats from Russia or radical Islamic terrorism. But while it has been in the shadows, the threat has only grown more dangerous."[22] By positioning the two nations in relation to one another, in a hierarchy anchored by terrorism, he amplifies the Chinese threat. Here, I consider three recurring racist and sexist representations of China as populated by individuals (1) who are devious and suspect, loyal only to their nation of origin; (2) whose way of being is effeminate and weak; and (3) who engage in economic espionage via cybercrime that threatens the United States. I maintain that the United States is comparatively soft on comparable or worse Russian violations partly due to their shared commitments to white supremacy. Geopolitically speaking, this casts Russia not as Edward Said's Orientalized Other but as Richard Dyer's "bad white."[23] The bad white is without a doubt a villain—but one that is familiar and sympathetic enough to allow "good whites" to position themselves as morally superior heroes among their own kind. Russia exemplifies a racial and moral gray area that breaks with ideal (colonial) foreign policy but facilitates the maintenance of white supremacy and aggressive masculinity. I show this by detailing how multiple stakeholders describe Russian saboteurs with (1) more generous attribution of motive, (2) more respect for raced and gendered strongman and mafioso behavior, and (3) more technological awe at infringing behaviors as compared to their Chinese counterparts. Chinese infringement is presented as uniquely threatening to global legal orders.

My argument proceeds in three parts. Part I outlines two theoretical frameworks for examining how racialization unfolds in the context of economic espionage specifically and intellectual property law generally: Critical Race Intellectual Property (CRTIP) and Third World Studies (TWS). CRTIP applies the intersectional insights of Critical Race Theory (CRT) to intellectual property to understand how race operates in the laws of copyright, patent, trademark, trade secret, unfair competition, and rights of publicity. TWS decenters the United States by considering how global liberation theories might approach the problems of racial and gender hierarchy in knowledge governance regimes. Intellectual property scholars relatedly speak of Third World Approaches to International Law (TWAIL) as a lens for thinking about the international inequities produced by Euroamerican knowledge ownership regimes.[24] Part II examines how China is racially represented and geopolitically managed in conversations about cybercrime and espionage in the larger context of histories and formations of Asianness. Part III considers how Russia is racially represented and geopolitically managed in conversations about hacking and disinformation in the larger context of the histories and formations

of whiteness. The conclusion posits that drawing upon feminist cyberlaw's articulations of ethics and fairness can help build equitable global racial orders of intellectual property that divest from whiteness.

RACE AND GLOBAL GEOPOLITICS

CRTIP is a term that Deidré Keller and I use to organize and describe a body of race and gender progressive intellectual property scholarship and activism from the past three decades that is largely authored by people of color.[25] We maintain that bringing CRT, the current racial boogeyman of the fascist right, together with intellectual property encourages intentional consideration of race as an organizing concept in a wide range of legal contexts. As we understand it, CRTIP functions as a set of questions that aid in drawing nuanced intersectional conclusions about the cultural and political superstructures of intellectual property regimes.[26] Like CRT, a set of principles and praxes for understanding how race remains entrenched in facially race neutral laws and addressing that embedded inequity, CRTIP focuses on where and how intellectual property law fails to produce racially just and racially equitable outcomes. As a theoretical lens, CRTIP is not confined to analyses of the United States or race. Asking questions about transnational intellectual property regimes and how they are deployed in the service of larger systems of colonialism can illuminate when and how punishment for violation of intellectual property norms is actually punishment for deviation from Euroamerican norms—for example, an implicit form of "intellectual property imperialism."[27] By making these interventions intersectionally, CRTIP can invoke and complement feminist cyberlaw's theorizations of fairness and equity.

Gary Y. Okihiro explains TWS as an interdisciplinary movement centered on finding commonality in the struggle for liberation.[28] Unlike Ethnic Studies and its progeny, which he maintains can produce divisive forms of identity politics, TWS is grounded in global solidarities.[29] I am interested in how TWS offers a path to reimagining knowledge governance regimes, around a wide range of transformative cultural values. I embrace the phrase "Third World" alongside "Global South" in this chapter as a means of calling upon histories of radical racial activism rooted in 1960s era frameworks of alliance in liberation,[30] as well as invoking the ideological and methodological imperatives of TWAIL.[31] James Gathii, who is interested in transformative justice approaches to international law, proposes that "there is an opportunity for learning, sharing, and collaboration between CRT and TWAIL scholars" that emphasizes both colonial extraction and white supremacy as meaningful analytics.[32] J. Janewa Osei-Tutu has compellingly applied TWAIL to intellectual property law by highlighting the need to decenter American epistemologies while focusing on equitable ownership and egalitarian access to knowledge across the globe.[33] This chapter draws upon the often intersecting approaches of CRTIP, TWS, and TWAIL scholars in intersectionally examining intellectual property's

racial orders, the logics of which implicitly and explicitly structure rhetorics around Russian and Chinese theft of trade secrets via cyberespionage.

THE FEMINIZED ASIANNESS OF CHINESE CYBERCRIME

In a recent article for the *South China Morning Post*, Leo Yu observed that ongoing Congressional investigations into Tik Tok as spying technology are rooted not in fact but in the "original sin" of Chinese ownership.[34] During the hearings, Republican Jay Obernolte asked accusatorily: "How could looking at the algorithm confirm that [Tik Tok is] free from foreign influence?"[35] while confrontationally informing CEO Shou Zi Chew "you are not trusted here."[36] Reasonable people may disagree about the nature and scope of the privacy issues associated with Tik Tok but the evidence that Chinese-owned companies are held to higher and racialized standards than white-owned ones is difficult to deny. A bipartisan majority of US policymakers appear committed to the narrative of China as a nation of disloyal spies, who mobilize new technologies in the service of global political and economic domination. Their prejudices are evident in the long history of actions intended to rein in Chinese trade secret theft that the National Counterintelligence and Security Center (NCSC), among other US government agencies, has characterized as "active and persistent."[37] While the NCSC's conclusion has its kernel of truth, the assumptions upon which it is based are troubling and hypocritical.

Multiple independent analyses of the China Initiative characterize it as a racist policy that targeted Chinese researchers for "relatively minor errors and omissions in grant applications, rather than spies stealing national security secrets or proprietary technology at the direction of the Chinese government."[38] A recent Brennan Center report historicizes the program, observing that "the FBI and Justice Department tendency to stretch facts and jump to conclusions in Chinese espionage cases pre-dated the China Initiative."[39] For instance, FBI counterintelligence training materials otherize those of Asian descent.[40] And earlier policies and actions, including the Economic Espionage Act of 1996 (EEA), reflect similar racial animus. The EEA, which turned theft of trade secrets into a federal crime,[41] marked an uptick in criminalizing previously accepted forms of competitive behavior, with an eye to Asia.[42] In 2022, the Stanford Center on China's Economy and Institutions noted that "[a] significant increase in the number of cases charging EEA-related offenses against suspects of Chinese heritage began in 2009 under the Obama administration."[43] The report goes on to propose that this is a symptom of disproportionate and racist targeting of Chinese people.[44] In a detailed review of the EEA, Andrew Chongseh Kim finds "significant disparities in the rates at which people of Asian descent are prosecuted for espionage and the outcomes of those prosecutions."[45] He concludes that "Chinese and other Asian defendants are twice as likely to be innocent as those of other races."[46]

This, of course, reinforces Del Visco's argument, that Sinophobic logics are reflexive in American political culture, including among Democrats.[47] CRT scholars and activists have long argued that "yellow peril" and "model minority" stereotypes organize American thinking about Asianness.[48] Within this binary, East Asians are presented as dangerous and disloyal "forever foreigners," who threaten to overrun the nation.[49] All too often, Asianness is also feminized, for instance through the association of spying with gossip and the association of disloyalty with weakness.[50] Such gendered tropes are evident in representations of the Chinese government as an all-powerful regime and Chinese citizens as eternally committed ideologues. Consider, for instance, the FBI's semi-fictional propaganda film, *The Company Man* (2015), which promotes yellow perilism by telling a story that contrasts a loyal American businessman with two disloyal Chinese cybercriminals in search of trade secrets. Circulated as a both an agency training video and public awareness campaign, *The Company Man* encourages multiple audiences to embrace American exceptionalism and Sinophobic paranoia.[51] The film tells a gendered, as well as raced, tale in which the dishonorable Chinese men, who shamelessly sneak around industrial spaces and offer exorbitant bribes, fail to live up to the honorable white masculinity of their American target.[52] As evident in the short film, representations of yellow perils and forever foreigners often feminize and emasculate East Asians,[53] representing them as obedient and cowardly automatons, dishonestly and submissively slinking through the shadows while sabotaging others and destroying relationships.[54]

Techno-Orientalism, Betsy Huang argues, emerged in the 1880s with descriptions of Asians as mechanistic alien bots without emotions.[55] In a longer history of the Asian as "model machine," a feminized robotic model of race, Long Bui highlights the many ways that US public culture consistently expresses ambivalence, specifically hate and reverence, about Asian technological prowess.[56] Though most often applied in science fiction studies, the term techno-Orientalism is useful in theorizing political rhetoric as well, specifically in highlighting how US trade, innovation, internet, and technology policy has collided with racial and gender anxieties. As Lok Sui and Claire Chun put it, "techno-orientalism . . . is the expressive vehicle . . . by which Western and Eastern nations articulate their fears, desires, and anxieties that are produced in their competitive struggle to gain technological hegemony through economic trade and scientific innovation."[57] They trace the concept of techno-Orientalism, through the work of David Morely and Kevin Robin, back to fears of Japanese technological superiority in the 1980s.[58] These fears played out in the VCR Wars, a series of conflicts over Asian production of video recording technologies that became lightning rods for national security and economic downturn rhetoric.[59] With respect to the former, the Supreme Court, in a decision that largely sidestepped the race and gender anxieties of the moment, held that the production and use of Betamax recorders did not constitute copyright infringement, only "time shifting" of programming that viewers

could watch at the originally scheduled time.[60] Still techno-Orientalism continued to rear its head, first in disputes over semiconductors and automobiles and later in disputes over cybercrime and platforms.

Despite the Supreme Court's decision, Motion Picture Association of America president Jack Valenti doubled down on the Japanophobic sentiments of the time. In 1982, he testified before Congress, at a hearing on home recording:

> "The single one American-made product that the Japanese, skilled beyond all comparison in their conquest of world trade, are unable to duplicate or displace or to compete with or to clone . . . this asset, [the US film and television production industry], which is unlike steel or silicon chips or motor cars or electronics of all kinds—a piece of sardonic irony that while the Japanese are unable to duplicate the American films by flank assault, they can destroy it by this video cassette recorder."[61]

This eerily familiar language expresses ambivalence about Japan, a nation "skilled beyond all comparison in the conquest of world trade," but nonetheless incapable of competing with America's creative moviemaking spirit. Technology operates as a tool of conquest in Valenti's analogy, as well as an anchor for racist and sexist intellectual property rights talk. War metaphors such as "flank assault" add a militant and patriotic urgency to the fight, with Japan engaging in feminized treachery and pathologized virality. Perhaps more importantly, they transform intellectual property rights talk into a raced and gendered conversation that disparages Japanese peoples' ability to produce artistic works and engage in war. The backhanded compliment that implicitly broadens copyright to include economic espionage, is discrimination deployed in the service of ownership rights.

The Japanophobia of the 1980s is intertwined with contemporary Sinophobia because, as Stanford Lyman puts it, anti-Asian racisms are overlapping and interchangeable, despite cultural and geopolitical differences: "The yellow peril appeared first as China, then as Japan, then as China and North Korea, then as China and Vietnam, then briefly as a temporarily prosperous Japan again, and, at the moment—once again as China."[62] Moreover, both are orientalist in their demonization of the so-called Orient as a means of validating Euroamerican white supremacy and legal regimes. Over time, the yellow peril narrative of the "Chinese copy" came to be treated as bipartisan fact, with the Bush Administration and the Clinton Administration cracking down on infringement, while bashing China's intellectual property policies. Under the Obama Administration, Biden declared: "Why have they not become [one of] the most innovative countries in the world? Why is there a need to steal our intellectual property? Why is there a need to have a business hand over its trade secrets to have access to a market of a billion, three hundred million people? Because they're not innovating."[63] This racist and gendered intellectual property rights talk is perpetually justified through moving goalposts: when China agrees to international norms, the US demands greater

compliance with its visions of knowledge ownership and economic norms.[64] Copying is treated as weakness not as resilience or choice.

America consistently shores up support for white supremacist intellectual property policies, including around trade secrets, through the mobilization of public emotions of fear and anger. These feelings are frequently rooted in national and geopolitical anxieties about the sustainability of the economy and whiteness.[65] But, as Sara Ahmed might contend, these "racial feelings" about employment, resources, and more are dishonest projections, defensive postures that ignore how the United States built its own economy on infringement and imposes double standards on other nations.[66] Indeed, good faith international intellectual property engagements require acknowledging the unique knowledge production trajectories and economic flows of nations in the Global South.[67] Yet according to US racial epistemes, Chinese people are quintessential bad intellectual property citizens who constitutionally refuse to comply with global norms, and Euroamerican nations are quintessentially good intellectual property citizens who intuitively steward international norms. These heroic myths of whiteness and masculinity are further normalized through relational racialization.

THE MASCULINE WHITENESS OF RUSSIAN HACKING

In 2020, CNN published an article with the headline "37 Times Trump Was Soft on Russia."[68] According to the article, Trump not only urged Russia to hack more, stating: "Russia, if you're listening, I hope you're able to find the 30,000 emails that are missing," he also proposed cybercrime cooperation with Putin.[69] The NCSC, in contrast to its assessments of China's economic espionage, describes Russia as a "sophisticated adversary," focused on military and economic domination.[70] While the Chinese threat originates in "persistence," a trope of mechanistic overrun, the Russian threat originates in "[sophistication]," a trope of elegant wrongdoing. If US policy toward China with respect to intellectual property and economic espionage can be characterized as condescending managerialism, its Russia policy can be described as begrudging acceptance. This hands-off approach has persisted for many years in the face of egregious violations of geopolitical norms, such as invasions of sovereign nations and interference in national elections, as well as a litany of intellectual property and economic espionage transgressions. This is curious given that cybersecurity experts consistently rank Russia in the top cybercrime threats to the US, alongside China. Russian hackers are described as "sowing chaos."[71] China's mechanistic precision is contrasted with Russia's thuggish coldbloodedness.[72] Yet the consequences for the two nations are very different.

Barron's reports that there are two primary reasons for US nonintervention in the latter issues: that Russia is careful to stay within applicable legal boundaries, here of infringement and cybercrime, and that the United States lacks the political will to enforce its policies. Vladimir Putin himself is aware that "there is

little Western countries have been willing to do to stop them . . . If there was little incentive in Russia to stop cybercrime before Ukraine, there is no incentive now.[73] Indeed, even when Putin declared, in March 2022, that Russian nationals would no longer be required to pay patent owners in "unfriendly countries," the US barely responded.[74] One of the few comparative studies of US treatment of Chinese and Russian infringement, a decades old essay, states what is now obvious: "In general, the United States has appeared to pursue different political, economic, and military goals in its relationships with Russia and China."[75] In practice, this means that the US has punished China for even those infractions that may fall under the gray areas of international law while permitting Russia to engage in similar acts with little more than a slap on the wrist.[76] The carte blanche that the United States has offered to Russia is entangled with white supremacy.

While the end of the Cold War produced détente with the US in the 1990s and 2000s, Putin's rise to power shifted the dynamic of the bilateral relationship.[77] The latter has been described as a "strongman," a term "historically deployed to describe autocrats who rule by violence and see themselves, or want to be seen, as worthy of fear."[78] Over the past twenty years, Putin has led an increasingly aggressive Russia, invested in transnational white supremacy. Indeed, multiple white nationalist leaders, including David Duke and Richard Spencer, have identified Putin's Russia as central to maintaining the global authority of whiteness.[79] Yet despite warnings about the destabilizing effects of Russia's white nationalism, the United States has declined to consistently condemn it.[80] I posit that this is largely because Russia, a "contingently white" country, has strategically exploited its whiteness in its geopolitical dealings.[81] The concept of contingent whiteness presupposes that race is produced through racialization, a process of constant change that explains "why certain groups become accepted as 'white,' how and why they adopt white identity claims, and what consequences those identity claims have for social relations."[82] Russia has endeavored to become whiter over time and Euroamerican nations have largely accepted this. Ian Law writes that "there have been striking changes in racial ideas, practices, exclusions and violence in Russia since the 1990s . . . the notion of a 'civilised country' has become a synonym for racial whiteness and Russianness a form of privileged whiteness."[83] Marina Levina observes that Russian investments in whiteness are used to reinforce what Jasbir Puar calls a "politics of debilitation"[84] on racially othered peoples such as Syrians and Ukrainians.[85] Russians choose whiteness because they benefit from its privileges, including relative impunity. The United States allows this because it benefits from Russia's whiteness, including regional counterbalancing.

Despite its chosen and bestowed whiteness, Russia has retained its long-standing identity as a political foil and imperial actor that requires containment. This is evident in multiple areas of friction with the United States, including discussions over NATO expansion. Conflict over intellectual property and economic espionage extends at least as far back to the Soviet Era when, as Debora Halbert observes,

national intellectual, political, and economic investments functioned as tools for proving cultural and artistic superiority.[86] Yet the contemporary American refusal to hold Russia accountable for its misdeeds suggests that the ideological dispute is embedded within a larger context. I propose that, while Russians continue to operate as "bad whites"[87] against whom Americans can demonstrate their global moral authority via soft power, it is also beneficial for the United States to engage in performative admonishments instead of meaningful consequences. Three racial outcomes flow from the toothless US response to Russia: (1) it normalizes the US position as the heroic "good white"[88] who appears to seek justice in the global arena; (2) it allows the United States to chastise Russia while also simultaneously colluding with Putin; and (3) it positions China below Russia in a divide-and-conquer style intellectual property and economic espionage racial order. US intellectual property rights talk with Russia thus supports larger architectures of white supremacy by letting the former off the hook while simultaneously deriding China for its illegal and illicit acts. It also exemplifies how realpolitik itself is constituted relationally, through categories of race and gender.

Returning to EEA data with this context around Russia illustrates how the United States uses intellectual property rights talk to reinforce Sinophobic racial hierarchies through relational racialization. The Stanford Center on China's Economy and Institutions notes that "Chinese-named defendants were 13.2% more likely to have their [EEA] cases dismissed or acquitted compared to other defendants, and 13.5% less likely to be found guilty of EEA-related charges than defendants with non-Chinese names."[89] In terms of sentencing, "Chinese-named defendants on average received 12.5 months longer jail terms compared to all other defendants and 12.4 months longer jail terms compared to defendants with Western names.[90] The targeting of Chinese defendants relative to other defendants is even more stark when considered over time. The number of Western defendants has declined from 59 percent of the total of all defendants in 1996–2008 to 28 percent of the total defendants in 2016–2020.[91] In comparison, approximately 50 percent of the total defendants prosecuted since 2009 have been Chinese.[92] These numbers are particularly notable given that Russian actors are growing increasingly bold. "US intelligence officials do not . . . rate China as the biggest threat to the US in cyberspace. The Russians are definitely better, almost as good as we are,' said one," Richard Clarke and Robert Knake reported in 2010.[93]

The Obama Administration and Biden Administration both imposed sanctions against Russia for engaging in economic espionage via cybercrime.[94] However, those sanctions were narrow and limited, especially compared to those imposed upon China.[95] The racialized rhetorics that American policymakers use to talk about Russia provide some insight about why the US shows this geopolitical rival such deference. A 2009 report released by the Rand Corporation describes Russia as a literal host and harbor for cybercrime, emphasizing that infringers use Russian websites to sell pirated and counterfeited goods because they operate as

"protected spaces for crime to arise."[96] Instead of being intertwined with narratives of threatening criminality like Black mafia rhetorics,[97] or narratives of devious yellow perils like Asian mafia rhetorics,[98] Russian mafia rhetorics suggest a worthy, masculine, strongman foe. Russian hackers are managers of the infringement world, whose ingenuity and infrastructure helps exceptional fakes to circulate. In 2008, Former Attorney General Michael Mukasey declared: "A Russian mobster selling fake handbags through a middleman in New York may also be selling pirated DVDs in London, counterfeit AIDS medication in Africa, and child pornography over the internet."[99] The "Russian mobster" is the protagonist of the story, here because he manages the sale of multiple goods. In 2006, the *Los Angeles Times* proclaimed, in an article entitled "Russians Able to Fake It Like No One Else," that "if there is a world capital of audacious fabrication, it must be Moscow, where fake is never a four-letter word."[100] It went on to describe Russian copies through "the French notion of *faire montrer* [sic]," noting "it's better to look like something than to be something. It's a very Eastern way of thinking."[101] Fakes may be Eastern, but Russian fakes are exceptional, certainly better than those Made in China. This racialized rhetoric of expertise positions Russia as strong and China as weak. Invoking France moves Russia closer to Europe—and whiteness.[102]

DECONSTRUCTING INTELLECTUAL PROPERTY'S RACE AND GENDER HIERARCHIES

This chapter has focused on how US intellectual property rights talk around economic espionage, trade secrets, and cybercrime prosecution uses comparative racialization, with gendered elements, as a means of justifying and enforcing inequitable knowledge governance policies. When speaking about China, the United States employs intellectual property rights talk that plays on fears of feminized yellow perils associated with racial deficiencies, viral replication, and overwhelming numbers. When speaking about Russia, the United States employs intellectual property rights talk that plays on respect for strongman mafiosos operating cybercrime rings to build and sell counterfeit goods. Russian hackers are imagined as deft and capable emblems of white masculinity even though, as Ruth Ben-Ghiat observes, they "are actually weak and insecure individuals but they appear [to supporters in] their countries as saviors, defenders, sex symbols at times, and other male archetypes."[103] Asian cybercriminals, unlike their white counterparts, are presented as femininely devious, thus undeserving of an empathetic counternarrative, despite their nations facing centuries of extractive colonialism.

US policies toward China and Russia are anything but independent. Their race and gender contrasts amplify one another while also reinforcing whiteness, a "relatively uncharted territory that has remained invisible as it continues to influence the identity of those both within and without its domain."[104] CRTIP, TWS, and TWAIL are useful intersectional tools for deconstructing intellectual property

rights talk because they make racial and gender hierarchies visible. Those using these methods would benefit from applying and deepening feminist cyberlaw's insights about ethics and fairness in the area of theft of trade secrets via cyberespionage as part of their theoretical inquiries. Doing so will not only highlight the intersectional race issues that arise with respect to the theft of trade secrets but also aid in building more equitable knowledge governance regimes with evenhanded application of laws and policies across racial groups.

NOTES

My gratitude to Amanda Levendowski and Meg Leta Jones for the opportunity to contribute to this groundbreaking collection and Hayley Behal for her adept research assistance on this project. Thank you as well to Jeremy Wu, Sharon Sandeen, and Peter Yu for their thoughtful input on this piece. I had the privilege of presenting an early version of this work at the Symposium on Trade Secrets for Scholars and Practitioners, organized by Nicola Searle.

1. Jeff Sessions, "Attorney General Jeff Sessions Announces New Initiative to Combat Chinese Economic Espionage," *The United States Department of Justice* (Nov. 1, 2018), https://www.justice.gov/opa/speech/attorney-general-jeff-sessions-announces-new-initiative-combat-chinese-economic-espionage. The US has passed no equivalent law to target Russia.

2. Katie Benner, *Justice Department Is Set to Modify Trump-Era Program Aimed at Fighting Chinese Threats*, NY Times (Feb. 20, 2022), https://www.nytimes.com/2022/02/20/us/politics/justice-department-china-trump.html.

3. Bethany Allen-Ebrahimian, *DOJ's China Initiative Under Scrutiny as Cases Fall Apart*, Axios (Jan. 25, 2022), https://www.axios.com/justice-department-china-initiative-scrutiny-41113cf0-14a8-42b9-9ba3-074446239bbf.html.

4. Spencer K. Turnbull, *Wen Ho Lee and the Consequences of Enduring Asian American Stereotypes*, 7 UCLA Asian Pac. Am. L.J. 72 (2001).

5. Ellen Barry & Katie Benner, *U.S. Drops Its Case Against M.I.T. Scientist Accused of Hiding China Links*, NY Times (Jan. 20, 2022) https://www.nytimes.com/2022/01/20/science/gang-chen-mit-china-initiative.html; Matt Schiavenza, *How the China Initiative Went Wrong*, Foreign Policy (2022), https://foreignpolicy.com/2022/02/13/china-fbi-initiative-spying-racism/.

6. Allen-Ebrahimian, *supra* note 3.

7. Benner, *supra* note 2.

8. Turnbull, *supra* note 4.

9. Stephen Del Visco, *Yellow Peril, Red Scare: Race and Communism in National Review*, 42 Ethnic & Racial Studs. 626 (2019) (illustrating how the *National Review* trafficked in fearmongering about those of Asian descent as a way of producing political unity among conservatives).

10. Eileen Guo, Jess Aloe & Karen Hao, *The US Crackdown on Chinese Economic Espionage Is a Mess. We Have the Data to Show It.*, MIT Tech. Rev. (2021), https://www.technologyreview.com/2021/12/02/1040656/china-initative-us-justice-department/.

11. Benner, *supra* note 2.

12. George Pence, *While China Initiative May Have Ended, Foreign Influence Remains DOJ Enforcement Priority*, Reuters (Mar. 28, 2022), https://www.reuters.com/legal/legalindustry/while-china-initiative-may-have-ended-foreign-influence-remains-doj-enforcement-2022-03-28/.

13. Mary Ann Glendon, Rights Talk: The Impoverishment of Political Discourse (2008).

14. For a detailed discussion of how these laws are unfairly leveraged against China, *see* Peter Yu, *Trade Secret Hacking, Online Data Breaches, and China's Cyberthreats*, 2015 CARDOZO L. REV. DE-NOVO 130 (2015).

15. Former Cybersecurity and Infrastructure Security Agency Director Chris Krebs linked Chinese hacking, patent theft, and public health in justifying the need for harsher legal penalties for cybercrime. Amanda Macias, "Former Cybersecurity Chief says Russia, China, Iran, and North Korea Are Trying to Steal Coronavirus Vaccine IP," *CNBC* (Dec. 6, 2020), https://www.cnbc.com/2020/12/06/former-top-cybersecurity-chief-says-russia-china-iran-and-north-korea-are-trying-to-steal-coronoavir.html; *see also* Nicole Sganga, "Chinese Hackers Took Trillions in Intellectual Property from About 30 Multinational Companies," *CBS News* (May 4, 2022), https://www.cbsnews.com/news/chinese-hackers-took-trillions-in-intellectual-property-from-about-30-multinational-companies/ (citing FBI Director Christopher Wray in linking Chinese cybercrime and industrial espionage with intellectual property theft).

16. Natalia Molina, *Understanding Race as a Relational Concept*, 1 MOD. AM. HIST. 101 (2018).

17. *See generally* Ian Haney López, DOG WHISTLE POLITICS: STRATEGIC RACISM, FAKE POPULISM, AND THE DIVIDING OF AMERICA (2022).

18. Glendon, *supra* note 13.

19. *See e.g.*, Madhavi Sunder, *IP3*, 59 STAN. L. REV. 257 (2006).

20. ANJALI VATS, THE COLOR OF CREATORSHIP: INTELLECTUAL PROPERTY, RACE, AND THE MAKING OF AMERICANS (2020).

21. *See e.g.*, Sessions, *supra* note 1.

22. *Id.*

23. RICHARD DYER, WHITE: ESSAYS ON RACE AND CULTURE, 35 (1997).

24. Athena D. Mutua, *The Rise, Development and Future Directions of Critical Race Theory and Related Scholarship*, DENV. U. L. REV. 339 (2006).

25. Anjali Vats & Deidré A. Keller, *Critical Race IP*, 36 CARDOZO ARTS & ENT. L.J. 735 (2018).

26. *Id.*

27. Alpana Roy, *Copyright: A Colonial Doctrine in a Postcolonial Age*, 26 COPYRIGHT REP. 112 (2008); *see also* Lateef Mtima, *What's Mine Is Mine but What's Yours Is Ours: IP Imperialism, the Right of Publicity, and Intellectual Property Social Justice in the Digital Information Age*, 15 SMU SCI. & TECH. L. REV. 323 (2012).

28. GARY Y. OKIHIRO, THIRD WORLD STUDIES: THEORIZING LIBERATION, 2 (2016).

29. *Id.*

30. *Id.*

31. Mutua, *supra* note 24.

32. James T. Gathii, *Writing Race and Identity in a Global Context: What CRT and TWAIL Can Learn From Each Other*, 65 UCLA LAW REVIEW 1610, 1612 (2021).

33. J. Janewa Osei-Tutu, *Denying Cultural Intellectual Property: An International Perspective on Anjali Vats's The Color of Creatorship*, 55 NEW ENG. L. REV. 79 (2020).

34. Leo Yu, *TikTok Is Targeted in the US for Being Chinese, Not For What It Has or Has Not Done*, SOUTH CHINA MORNING POST (Mar. 26, 2023), https://www.msn.com/en-xl/news/other/tiktok-is-targeted-in-the-us-for-being-chinese-not-for-what-it-has-or-has-not-done/ar-AA194p7j (accessed Mar. 29, 2023); *see also* Leo Yu, *From Criminalizing China to Criminalizing the Chinese*, 55 COLUM. HUM. RTS L. REV. (forthcoming 2024).

35. Gopal Ratnam, *Obernolte, Johnson Use Tech Backgrounds to Question Tik Tok CEO*, ROLLCALL (Mar. 8, 2023), https://rollcall.com/2023/03/28/obernolte-johnson-use-tech-backgrounds-to-question-tiktok-ceo/.

36. Yu, *supra* note 34.

37. *Foreign Economic Espionage in Cyberspace*, National Counterintelligence and Security Center, 2018, https://irp.fas.org/ops/ci/feec-2018.pdf.

38. Michael German & Alex Liang, *End of Justice Department's "China Initiative" Brings Little Relief to U.S. Academics*, Brennan Ctr. for Just. (2022), https://www.brennancenter.org/our-work/analysis-opinion/end-justice-departments-china-initiative-brings-little-relief-us.

39. *Id*.

40. *Id*.

41. Hanming Fang & Ming Li, *Racial Profiling Under the Economic Espionage Act*, Stan. Ctr. on China's Econ. & Insts. (2022), https://sccei.fsi.stanford.edu/china-briefs/racial-profiling-under-economic-espionage-act.

42. Julia Jayne and Ashley Riser, *Theft of Trade Secrets: The Economic Espionage Act, China Initiative, and Silicon Valley*, The Champion (Sept./Oct. 2019), https://www.nacdl.org/Article/SeptOct2019-TheftofTradeSecretsTheEconomicEspionag.

43. Fang and Li, *supra* note 41.

44. *Id*.

45. Andrew Chongseh Kim, *Prosecuting Chinese Spies: An Empirical Analysis of the Economic Espionage Act*, 40 Cardozo L. Rev. 749 (2018).

46. *Id*.

47. Dexter Roberts, *Biden Makes a Habit of Dissing Chinese Innovation*, Bloomberg Businessweek (2014), https://www.bloomberg.com/news/articles/2014-05-29/biden-makes-a-habit-of-dissing-chinese-innovation.

48. Yuko Kawai, *Stereotyping Asian Americans: The Dialectic of the Model Minority and the Yellow Peril*, 16 How. J. Commc'ns 109 (2005).

49. Mia Tuan, Forever Foreigners or Honorary Whites?: The Asian Ethnic Experience Today (1999).

50. *See e.g.*, Marika Cifor, *Acting up, Talking Back: TITA, TIARA, and the Value of Gossip*, 12 Inter-Actions: UCLA J. of Educ. and Info. Stud. 1 (2016); Joseph Cheah and Grace Ji-Sun Kim, Theological Reflections on "Gangnam Style": A Racial, Sexual, and Cultural Critique (2014).

51. Federal Bureau of Investigation, *The Company Man: Protecting America's Secrets* (2015), https://www.fbi.gov/video-repository/newss-the-company-man-protecting-americas-secrets/view.

52. Cifor, *supra* note 50.

53. *See e.g.*, Michael Park, *Asian American Masculinity Eclipsed: A Legal and Historical Perspective of Emasculation Through US Immigration Practices*, 8 Mod. Am. 5 (2012–2013).

54. Long T. Bui, Model Machines: A History of the Asian as Automaton, 2 (2022).

55. Betsy Huang, *Premodern Orientalist Science Fictions*, 33 MELUS (2008).

56. Bui, *supra* note 54.

57. Lok Siu & Claire Chun, *Yellow Peril and Techno-Orientalism in the Time of Covid-19: Racialized Contagion, Scientific Espionage, and Techno-Economic Warfare*, 23 J. Asian Am. Stud. 421 (2020).

58. *Id*.

59. James Lardner, Fast Forward: Hollywood, the Japanese, and the Onslaught of the VCR (1987).

60. Sony Corp. of America v. Universal City Studios, Inc., 464 U.S. 417 (1984).

61. *Home Recording of Copyrighted Works: Hearings Before the Subcommittee on Courts, Civil Liberties, and the Administration of Justice of the Committee on the Judiciary*, 97th Cong. (1981) (testimony of Jack Valenti), https://cryptome.org/hrcw-hear.htm.

62. Stanford M. Lyman, *The "Yellow Peril" Mystique: Origins and Vicissitudes of a Racist Discourse*, 13 Int'l J. Pols., Culture, & Soc'y 683 (2000).

63. Roberts, *supra* note 47.

64. Yu, *supra* note 14.

65. *See e.g.*, Michelle Murray Yang, *At War with the Chinese Economic Yellow Peril: Mitt Romney's 2012 Presidential Campaign Rhetoric*, 45 J. Intercultural Commc'n Rsch 45 (2016).

66. Sara Ahmed, *Affective Economies*, 22 Social Text 117 (2004).

67. *See e.g.*, Rosana Pinheiro-Machado, Counterfeit Itineraries in the Global South: The Human Consequences of Piracy in China and Brazil (2017).

68. Marshall Cohen, *37 Times Trump Was Soft On Russia*, cnn (Nov. 11, 2019), https://www.cnn.com/2019/11/17/politics/trump-soft-on-russia/index.html.

69. *Id*.

70. *Foreign Economic Espionage in Cyberspace, supra* note 37.

71. Joseph Marks, *Analysis | Is Russia or China the Biggest Cyber Threat? Experts Are Split*, Washington Post (Jan. 20, 2022), https://www.washingtonpost.com/politics/2022/01/20/is-russia-or-china-biggest-cyber-threat-experts-are-split/.

72. *Id*.

73. *Id*.

74. Helen Holmes, *Putin's War on Intellectual Property Has Only Just Begun*, Observer (Mar. 17, 2022), https://observer.com/2022/03/putins-war-on-intellectual-property-has-only-just-begun/.

75. Connie Neigel, *Piracy in Russia and China: A Different US Reaction*, 63 L. & Contemp. Probs. 179 (2000).

76. *Id*.

77. Stephen Handelman, *The Russian "Mafiya,"* Foreign Affairs, March 1, 1994, https://www.foreignaffairs.com/articles/russia-fsu/1994-03-01/russian-mafiya.

78. Daniel King, *There Are Many Words for Vladimir Putin. Is He Still Your "Strongman"?*, Mother Jones (Feb. 27, 2022), https://www.motherjones.com/politics/2022/02/there-are-many-words-for-vladimir-putin-is-strongman-one/.

79. Elizabeth Grimm Arsenault & Joseph Stabile, *Confronting Russia's Role in Transnational White Supremacist Extremism*, Just Sec'y (Feb. 6, 2020), https://www.justsecurity.org/68420/confronting-russias-role-in-transnational-white-supremacist-extremism/.

80. *See e.g.*, Cohen, *supra* note 68.

81. Vic Satzewich, *Whiteness Limited: Racialization and the Social Construction of "Peripheral Europeans,"* 33 Social Hist. 271 (2000).

82. *Id*. at 273.

83. Ian Law, *Review of Attaining Whiteness. A Sociological Study of Race and Racialisation in Russia*, 51 Sociologisk Forskning 87 (2014).

84. Jasbir Puar, The Right to Maim: Debility, Capacity, Disability (2017).

85. Marina Levina, *Epidemiology as Methodology: COVID-19, Ukraine, and the Problem of Whiteness*, 19 Commc'n & Critical/Cultural Studs. 112, 114–17 (2022).

86. Debora J. Halbert, The State of Copyright: The Complex Relationships of Cultural Creation in a Globalized World (2014).

87. Dyer, *supra* note 23.

88. *Id*.

89. Fang and Li, *supra* note 41.

90. *Id*.

91. *Id*. The remaining categories—Other Asian, Hispanic, Middle Eastern, Unknown, and Firm—are inapplicable to Russia.

92. *Id*.

93. Richard A. Clarke and Robert Knake, Cyber War: The Next Threat to National Security and What To Do About It, 34 (2010). For instance, 74 percent of revenue from ransomware attacks goes to hackers linked to Russia. Joe Tidy, *74% of Ransomware Revenue Goes to Russia-Linked Hackers*, BBC (Feb. 14, 2022), https://www.bbc.com/news/technology-60378009.

94. Marcus Lu & Christina Kostandi, *A Recent History of U.S. Sanctions on Russia*, Visual Capitalist (2022), https://www.visualcapitalist.com/history-us-sanctions-on-russia/.

95. Steve Ranger, *Can Russian Hackers Be Stopped? Here's Why It Might Take 20 Years*, TechRepublic (2018), https://www.techrepublic.com/resource-library/downloads/can-russian-hackers-be-stopped-here-s-why-it-might-take-20-years-cover-story-pdf/.

96. Gregory F. Treverton et al., Film Piracy, Organized Crime, and Terrorism, Rand Corporation (2009).

97. Vats, *supra* note 20.

98. *See e.g.*, Mike Dillon, *The Immigrant and the Yakuza: Gangscapes in Miike Takashi's DOA*, Studies in the Humanities (June 1, 2012), https://www.proquest.com/docview/1539524714?pq-origsite=primo.

99. Michael Mukasey, *Remarks Prepared for Delivery by Attorney General Michael B. Mukasey at the Tech Museum of Innovation*, US Department of Justice (Mar. 28, 2008), https://www.justice.gov/archive/ag/speeches/2008/ag_speech_080328.html.

100. Kim Murphy, *Russians Able to Fake It Like No One Else*, Seattle Times (July 15, 2006), http://seattletimes.com/html/nationworld/2003128478_fakerussia15.html.

101. *Id*.

102. Vats, *supra* note 20.

103. King, *supra* note 77.

104. Thomas Nakayama and Robert Krizek, *Whiteness: A Strategic Rhetoric*, 81 Q. J. of Speech 291–301 (1995).