Centering Race in Analyses and Practices of Countersurveillance Advocacy
Mythologies of the Racialized Other in the Crypto Wars

Karina Rider
Postdoctoral Researcher
Microsoft Research New England

S.L. Revoy
Independent Scholar

Citation: Rider, Karina and S.L. Revoy. 2022. "Centering Race in Analyses and Practices of Countersurveillance Advocacy: Mythologies of the Racialized Other in the Crypto Wars." In *Privacy: Algorithms and Society* (ed. M. Filimowicz). New York: Routledge.

Introduction

In 2016, Karina attended an international conference called RightsCon. The annual gathering brought together technologists, activists, scholars, and policymakers to discuss issues pertaining to digital technologies, human rights, and civil liberties. Just before lunch on the second day, Karina attended a panel titled "Witnessing Police Violence, On and Off the Internet," organized by Morgan Hargrave with WITNESS; Taina Angeli Vargas with the Ella Baker Center; and Malkia Devich-Cyril from the Center for Media Justice (now MediaJustice). The panelists addressed questions regarding activists' fight against state surveillance. How can activists—especially those fighting police brutality—defend themselves against surveillance when they are often unaware of the kinds of technologies that the state has at their disposal? Devich-Cyril had this to say about these questions:

> To some degree, I think that people know that they're being surveilled. We know that, right? Young people in particular are aware that they have to code their language and code their interactions online […] And I don't mean code the way y'all mean code. And I don't mean encrypt the way y'all mean encrypt. But, like, how we protect and hide what we are talking about, and who we're talking to, and all those kinds of things. Can I just say, as an aside, I think that it's interesting that the encryption debate is so—it's so lodged within this wonky—if I might say—white, techy world, when in fact people of color been encrypting for generations, you know what I'm saying? People of color know all about encryption and how to code.

Although Devich-Cyril acknowledges that encryption can provide a layer of security for people of color at risk of violence and harassment—at one point arguing that Twitter needs to do more to ensure users' safety by encrypting direct messages on the platform—they also criticize the narrow, essentialist understanding of encryption which permeates tech circles. By characterizing debates about encryption as being "lodged" within a "white, techy world," Devich-Cyril draws attention to how many technologists have a limited understanding of the relationship between technology and social justice; in particular, they are unaware of (or downplay) how people of color have developed tactics over generations to protect themselves from violence and create safe spaces through analogical forms of encryption, such as coded speech. Instead, they conceptualize encryption as a circumscribed technolegal intervention detached from analyses of how surveillance is structured by racism and white supremacy.

Devich-Cyril's discussion provides a generative entry point for thinking through the ambivalence of encryption. On the one hand, encryption can be crucial in situations where activists—many of them people of color, queer, and/or undocumented—are at risk of violence from individuals, organized groups, and the state. On the other hand, as Devich-Cyril points out, activists and technologists can overestimate the power of encryption to ensure safety on its own; minimize the importance and sophistication of tactics people of color have developed over generations; and ignore how surveillance disproportionately targets people of color.

This chapter contributes to research on countersurveillance advocacy by troubling our assumptions about encryption's universal ability to protect vulnerable groups from state violence, while building on scholars' and activists' arguments that encryption debates frequently ignore questions of race. Rather than presuppose encryption as a counter-surveillant, pro-privacy technology which can be implemented to protect groups from the state (what West [2020] calls determinist conceptualizations of encryption), we explore how encryption has served as a space for negotiating the competing logics of mass incarceration and neoliberal economic development—logics which are fundamentally structured by race. By examining popular, mythological conceptions underscoring encryption policy debates and reconsidering them as constitutive of a space of frequently racialized state violence, we aim to demonstrate to scholars and digital rights advocates the importance of centering race in countersurveillance advocacy and research. Doing so can trouble existing assumptions about encryption while generating new questions for future research.

Throughout this chapter we present findings from a discourse analysis of federal encryption policy debates from 1990-2016. During this period policymakers and members of the law enforcement and intelligence communities aggressively advocated for encryption regulation in the form of mandatory decryption capabilities; state actors set the terms of the debate as being not about whether the federal government *should* be able to demand decryption, but rather what the most efficient and palatable options were for designing such a capability: the state or private manufacturers. The most infamous of these proposals is the Clipper Chip, a cryptographic device to be embedded into telephones and other devices sold by American companies that would afford law enforcement the ability to decrypt communications. Companies and digital rights activists

pushed back against these proposals, arguing that encryption should be deregulated—at the time, federal law prohibited U.S. companies from exporting products with encryption—so that American companies could flourish in emerging global markets for IT products and, in the process, protect user privacy through self-regulation. Our analysis demonstrates that these policy debates were fundamentally structured by mythological constructions of racialized others by (a) the state, which conjured myths of violent, sexual deviants to push for encryption regulation, and (b) the market, which drew upon nascent anxieties about foreign governments overpowering the U.S. because of globalization. Eventually the two sides came to a compromise: the Clinton administration dropped its proposals for mandatory decryption while lifting export controls, allowing U.S. companies to sell their IT products abroad. At the same time, however, they organized informal, backroom deals in which companies agreed to provide law enforcement with access to their customers' encrypted communications. This created a situation wherein racialized populations were caught in a discursive double-bind between the exclusionary demonizing practices inherent in myths used to justify encryption regulation (and, by extension, the carceral institutions bolstered by mandatory decryption) and resulting practices of predatory inclusion in which people of color are included in American companies' user bases and subjected to racialized surveillance as a result.

In the first section, we explore research on encryption as a tool for protecting privacy and countering surveillance, highlighting the different ways in which advocates and scholars have presented a narrow conceptualization of encryption which ignores questions of race. The following section presents the findings of our empirical investigation of federal policy debates over encryption from 1990-2016: first, how policymakers as well as police and intelligence officials habitually invoke mythological constructions of racialized criminal figures in order to advocate for encryption regulation and how corporations responded by stoking fears about a possible globalization not led by the U.S., but by foreign countries such as China, employing in their own way a different mythological figure of the threatening racial Other. The next section situates these findings in recent explorations of the co-construction of racial capitalism and network capitalism; here, we argue that deregulating encryption is a crucial step in setting the stage for future processes of predatory inclusion (Cottom 2020). We conclude by emphasizing the importance of accounting for race when researching and advocating for technologies

assumed to be universal counter-surveillance tools. Despite the centrality of racialized mythological figures to encryption policy debates, digital rights advocates left the carceral and neoliberal logics untouched. This represents an opportunity moving forward; continuing encryption policy debates can provide technical experts, countersurveillance advocates, and scholars a space to contest ongoing racism in the United States.

Encryption and Counter-Surveillance Advocacy

Without a doubt, encryption is a critical tool for vulnerable populations trying to protect themselves from violence and harassment, whether from organized groups, individuals, or governments. A 2015 report from David Kaye, the UN special rapporteur on freedom of expression, draws a direct link between encryption and freedom of expression, opinion, and the right to receive information and ideas. According to the report, encryption can "provide individuals and groups with a zone of privacy online to hold opinions and exercise freedom of expression without arbitrary and unlawful interference or attacks" (Kaye, 2015, p. 7). This is particularly important for civil society groups and individuals who are victims of "targeted surveillance, distributed denial of service attacks, and online and offline intimidation, criminalization and harassment […] Encryption and anonymity enable individuals to avoid or mitigate such harassment" (Kaye, 2015, p. 8). Kaye's conceptualization draws from a "cryptographic imaginary" constructed by digital rights advocates that links encryption to democratic values by "establishing that encryption may be a precondition for democratic self-expression and association, by fostering zones of privacy where communities of individuals can join together without fear of surveillance" (West, 2018, p. 11). It follows, then, that in order to ensure civil society organizations and individuals have access to strong encryption, the IT firms which build, run, and service the majority of our communication channels need to be pressured into encrypting user data by default. Following the Snowden disclosures in 2013, many American companies—such as Apple and Google—faced mounting pressure from users and digital rights advocates to strengthen encryption in their products (McLaughlin, 2015).

However, focusing advocacy efforts on petitioning tech firms to change their products can legitimize corporations as protectors of the common good as well as the de facto providers of social services. In their study of submissions made to Parliament concerning the draft

Investigatory Powers Bill in the United Kingdom, Stevens and Allen-Robertson (2021) found that civil liberties groups, digital rights organizations, and corporations tended to conflate encryption and human rights when opposing the bill. The problem with this conflation is that "the technology industry is thus utilising its privileged position as providers of encryption technologies to conflate their own activities with human rights protection, and to frame their data-driven activities of 'surveillance capitalism' [Zuboff, 2015] as innocuous and distant from state surveillance practices" (Stevens and Allen-Robertson, 2021: 2). Similarly, Gürses et al. (2016, p. 586) note that, despite the Snowden disclosures being "disastrous for the reputations of major tech corporations," they have been able to recuperate some of the damage because "the deployment encrypted services can now serve as the basis of public relations campaigns. The idea that solutions to societal problems can come from technical progress and sophistication in the private sector is the bread and butter of Silicon Valley corporations." Framing the problem of government surveillance as something which can be addressed using corporate technologies means that advocates are inadvertently legitimizing tech firms as the natural providers of social goods.

In addition to positioning American tech firms as providers of social goods, scholars have argued that digital rights advocacy often provides a narrow understanding of encryption as an intervention into a technolegal problem, a tendency that has several consequences. First, there is evidence that the narrow framing of encryption as ipso facto a technolegal intervention against government overreach obstructs activists' ability to build broad coalitions across issue areas—particularly those concerned with racial inequality—which is only becoming more crucial as digital technologies saturate our institutions and everyday lives. In their interviews with a range of activists following the Snowden disclosures, Dencik et al. (2016) found little overlap between digital rights groups focused on technolegal interventions, including encryption, and other social justice organizations. Aouragh et al. (2015) similarly argue that the division of labor between activists and technical developers must be overcome to develop true alternatives to the commercial platforms the former frequently rely on for organizing.

Second, encryption advocacy frequently ignores the ways in which surveillance is fundamentally structured through intersecting lines of race, class, gender, ability, and nationality. For example,

advocates often frame the problem of government surveillance as having to do with the scope of data collection; the problem, they argue, is that all individuals are under suspicion, rather than the few who should be investigated (Gürses et al., 2016). This framing establishes a problematic demarcation between mass and targeted surveillance, with the latter being implicitly (or sometimes explicitly) held up as the desirable state of affairs. Therefore:

> these discussions fail to give space to those who are on the receiving end of global surveillance programs and linked forms of violence, such as extrajudicial killing, torture, and impoverishment including populations in the United States and Europe whose racialization has been integral to histories of colonialism, plantation slavery, and empire. (Gürses et al., 2016, p. 577).

In general, technolegal framings of interventions into surveillance tend to be depoliticizing. Although activists often face pressure to frame their arguments in terms their targets will find acceptable—for instance, by arguing to cash-strapped local governments that mass surveillance is expensive—to achieve their goals, doing so can also "[limit] our understanding of the implications of these data-driven practices that underpin contemporary surveillance and [dilute] their politicized nature" (Dencik et al., 2016, p. 8).

To remedy these shortcomings, scholars have proposed new frameworks which center analyses of racism and white supremacy. Rexhepi (2016, p. 2) argues that "to unsettle, decenter and rethink veillance theories beyond the taxonomies of surveillance inside liberal democracies, a critical intervention needs to destabilize and disrupt sur/violence by shifting its focus from the center to the periphery." Simone Browne's work is a crucial step in this direction. Browne (2015) centers theorizing race and racism in thinking through the dynamics and consequences of both historical and contemporary surveillance. In doing so, Browne (2015, p. 8) develops the concept of *racializing surveillance*, in which "enactments of surveillance reify boundaries along racial lines, thereby reifying race, and where the outcome of this is often discriminatory and violent treatment." Racializing surveillance does not solely distribute harms along racial lines, but simultaneously shapes collective understandings of race.

Countersurveillance advocates also reproduce and reify understandings of race as they attempt to counteract state surveillance schemes. For instance, advocates frequently refer to George Orwell's *1984* as a quintessential example of the dystopian future we will inevitably realize if we

allow the government to engage in mass surveillance (Gürses et al., 2016). The problem is that Orwell tacitly depicts mass surveillance as normalized where non-Western countries are concerned due to his use of totalizing mass surveillance as the novum of his dystopian United Kingdom; relying on this novel to understand the dynamics of mass surveillance "undermine[s] a political reading that would attend to the racial, gendered, classed, and colonial aspects of the surveillance programs" being critiqued (Gürses et al., 2016, p. 577). The use of such touchstones, centered as they are on the threat of figures of the Other and their oppressive, immoral practices as counter to the intrinsic values of Western states, should attune us to the broader use of such mythological tropes when considering the real policy debates surrounding surveillance, such as the regulation and use of encryption technologies; this is quite evident in our discourse analysis. In the following section we therefore turn to a semiological treatment of the rhetoric of the Crypto Wars to help unveil the mythic representations of racialized populations which prove foundational for understanding the rhetorical tactics of both state and private sector actors as they negotiate the political reality of regulating encryption technology.

A Semiology of the Crypto Wars

Policy debates over encryption are often leavened with mythological language by all concerned to more provocatively ground arguments made by state actors for the intrinsic security risks of unfettered cryptographic technology and, conversely, those made by private sector actors for less restrictive regulations in order to maintain competitive advantage in the global market. The mythological language used is entirely premised on representing long-standing, totemic figures which encapsulate deviant stereotypes common of racialized populations, rearticulated within the context of encryption, digital communication, and the security threats they represent. Here, we use mythology as articulated by Roland Barthes (1972, p. 114-5), for whom:

> [myth] is constructed from a semiological chain which existed before it: it is a second-order semiological system. That which is a sign (namely the associative total of a concept and an image) in the first system, becomes a mere signifier in the second. We must here recall that the materials of mythical speech […] are reduced to a pure signifying function as soon as they are caught by myth. Myth sees in them only the raw material; their unity is that they all come down to the status of a mere language. Whether it deals with alphabetical or pictorial writing, myth wants to see in them only a sum of signs, a global sign, the final term of a first semiological chain […] As a total of linguistic signs, the meaning of the myth has its own value, it belongs to a history […] The meaning is already

> complete, it postulates a kind of knowledge, a past, a memory, a comparative order of facts, ideas, decisions.

In brief, myth is generated when a pre-existent sign is associated with an artificed meaning for particular groups, places, and times via its successful assertion within the politics of a given milieu, thereby becoming successfully embedded and legible for certain cultures. The bespoke nature of myth means that its durability and reach is an idiosyncratic function of its cultural circulation. Myth is a constantly generative order of language, with new associations always being fabricated, some fading, and all having to constantly renew themselves to maintain their cultural legibility. When we are considering discourse, then, we must consider the way in which mythological knowledge, these ever-evolving and dynamic second-order semiotic associations circulating as part of the experience of language, serves as an influential component that must be confronted when considering the "problem of the 'discursive regime,' of the effects of power peculiar to the play of statements" (Foucault 2010, p. 55)

Myths regarding the Other are one of the most durable, indeed perennial, and influential forms of myth which circulate in human cultures. Such myths are so persistent in their various permutations that it is entirely possible that there is always "a set of people who, in one way or another, are regarded as pertaining to the foreigner, members of a surplus population, undesirables of whom one hopes to be rid" (Mbembe 2019, p. 42). The recitation of these myths regarding the other, the despised populations which may represent absolute threat and for whom "death has nothing tragic about it" and is "deprived of all symbolism" is the semiotic motor of what Achille Mbembe calls the necropolitical, an ascendant form of powers premised on the normalization of death for groups at the margins of society, whether by large-scale destruction of by "the strategy of 'small massacres' inflicted one day at a time, using an implacable logic of separation, strangulation, and vivisection, as we see in all the contemporary theaters of terror and counterterror" (Mbembe, 2019, p. 38). Each time a stereotype is successfully deployed in everyday or political speech, it is another mark of the necropolitical, as "racism is the driver of necropolitical principle insofar as it stands for organized destruction, for a sacrificial economy" (Mbembe, 2019, p. 38). When myths regarding the criminal nature of racialized populations are used to justify policy, and especially when they are effective, it not only signifies the potent renewal of that myth as a legible form of inferential language, but further drives the

necropolitical abuse of the subjects whose lives are rendered fodder for the promotion of state power.

It is difficult to overstate the role such myths play in the Crypto Wars. Within these debates, mythological language bridges the reciprocal, mutually reinforcing movement between older, pre-digital mythologies regarding perennial enemies of national and state security—the pantheon of contemporary criminal others who serve as the landscape of perceived threat in security debates—alongside an emergent mythology regarding the unprecedented dangers inherent in digital technologies. Myths concerning the fundamental insecurity of the commercialized internet buttress antecedent mythological concepts of racialized criminals, who are depicted in such arguments as naturally gravitating toward encryption to cover up their deviant, criminal (often violent and sexual) activities; conversely, the presumptive uptake of encryption by these archetypal enemies of the U.S. simultaneously underscores and augments the perceived threat of such technologies, doubly underlining the need for an extraordinary response to this alignment of old and new threats. For their part, private sector technology firms mobilized similar mythological language while constructing a different threat: that of the foreign country which could dominate economic globalization, becoming a threat to U.S. national security and its economic prosperity. Re-evaluating the rhetoric of the Crypto Wars through the lens of mythological archetypes and their mobilization reveals the Crypto Wars as yet another necropolitical theater which strategically leverages certain racialized populations as reductive archetypes to serve as discursive resources which aid in negotiating the expansion of state as well as private sector power and to reinforce both the legibility and potency of the archetypes themselves.

Proposals for Regulating Encryption: Mythologies of Domestic Criminals

The fear of racialized criminals using the capacities of the internet with unrestricted encryption is the overarching mythological construct guiding the arguments for the necessity of state intervention in the development of encryption technologies. Many state actors consistently depict encryption as fundamentally compromising law enforcement; Rep. Edward Markey, for example, questioned whether:

> technology is evolving at such a rapid pace that it has surpassed our ability to be able to provide the police with an adequate ability to be able to monitor, through legal court order, the conversations, the information which is being transmitted over these modern technologies. (Telecommunications Network Security, 1993).

Over the course of debates over encryption regulation, these theoretical concerns become increasingly framed as a concrete inevitability given the spread and saturation of digital technologies in different areas of life. As Robert Litt of the Department of Justice stated:

> I can't emphasize too strongly the danger that unbreakable, non-recoverable encryption poses: as we move further into the digital age, as more and more data is stored electronically rather than on paper, as very strong encryption becomes built into more and more applications, and as it becomes easier and easier to use encryption as a matter of routine, our national security and public safety will be endangered unless we act responsibly. (Privacy in the Digital Age, 1998)

The commercialization of the internet and its availability in more accessible, user-friendly forms, is used by Litt to argue that criminals of any technical sophistication will quickly be able to exploit cryptographic technologies to commit violent, organized (often sexual or drug-related) crime. The use of encryption by criminal groups who are historically racialized (cf. Kappeler and Potter, 2018) is not merely framed as an assault on the very capacity for law enforcement, but, because such interventions are always framed as fully legal and court-approved, "begins removing the power that society has given the courts," as the deputy director of the NSA, William Crowell, put it (Encryption, Key Recovery, and Privacy, 1997). In this view, the mere existence of unrestricted encryption constitutes an assault on the legal system and the state as such to determine legal search and seizure activities by law enforcement agencies, while practically "stripping law enforcement of their ability to successfully perform electronic surveillance, wiretaps, and the search and seizure of criminal information stored in computers," according to Gene Voegtlin of the International Association of Chiefs of Police (Encryption Security, 1999).

State representatives invoke a set of possible criminal activities that could occur via encrypted channels and, although debates about encryption policy in the internet era have lasted more than 30 years, the set remains remarkably stable. Between 1990-2016, state representatives claimed encryption was used by "terrorists, drug dealers, and other criminals" and "gang members [and] drug dealers" (Telecommunications Network Security, 1993); "drug traffickers, organized crime groups, major street gangs and terrorist groups", "criminal organizations", "criminal elements or

foreign agents", "sophisticated criminal[s]", and "well-organized, well-directed, well-motivated terrorist group[s] coming from abroad" (The Administration's Clipper Chip, 1994); "bad guys" and "terrorists, violent criminals, organized crime groups, and drug trafficking organizations, which are highly structured" (Communications and Computer Surveillance, 1994); "criminals, drug lords, and terrorists […] [and] their criminal associates" and "the People's Liberation Army of China" (Encryption Security, 1999); "the criminal element" and "a massive drug dealer, an arms trafficker, a child pornographer, or a child molester" (Going Dark, 2011); "pedophiles" (Federal Bureau of Investigation, 2011); "extremists" (Terrorism Gone Viral, 2015); and "criminal defendants in every jurisdiction of America" (Going Dark, 2015).

Furthermore, encryption was depicted as being used in the commission of crimes such as "gambling, prostitution, vice, just all sorts of crime" (Telecommunications Network Security, 1993); "the drug trade" (Encryption Security, 1999); "child abduction, child exploitation, prison escape, and other threats to public safety" (Going Dark, 2011); "child pornography" (Federal Bureau of Investigation, 2011); by ISIS to "recruit fighters, share intelligence, raise funds, and potentially plot and direct attacks undetected", to provide "advice for traveling to terror safe havens, contact information for smugglers in Turkey, or the membership process for joining ISIS itself," and as a "free zone by which to recruit, radicalize, plot, and plan" (Terrorism Gone Viral, 2015); and to "covertly plot violent robberies, murders, and kidnappings […] to establish virtual communities to buy, sell, and encourage the creation of new depictions of horrific sexual abuse of children" (Going Dark, 2015).

At the same time, however, state officials depicted those criminals who might use encryption as potentially dangerous, crafty, and highly organized and motivated, as also being "stupid" and "lazy." One of the most common criticisms of government surveillance proposals was that criminals, if faced with a choice between a cell phone with built-in police surveillance capabilities and one without, would obviously purchase the latter, or would simply add their own layer of encryption to obstruct government surveillance. In response, state officials explained that criminals would buy these surveillance-enabled devices regardless. William Reinsch, Undersecretary of Commerce, told Congress to "never underestimate the stupidity of some of the people we have to deal with" (Encryption Security, 1999). Valerie Caproni, FBI General

Counsel, made a similar comment over a decade later: “sometimes we want to think that criminals are a lot smarter than they really are. Criminals tend to be somewhat lazy, and a lot of times, they will resort to what is easy” (Going Dark, 2011). The seemingly contradictory characterization of criminals as being both “well-organized and highly-motivated” and “lazy” is not actually contradictory at all: it permits white Americans to fear racialized criminals while still believing in their own superiority and to have the confidence that law enforcement, if given enough power, can catch and incarcerate them.

These extreme views regarding the threat of malicious activity is rooted in a dual mythology regarding the internet, encryption, and highly capable criminals, whom Paul Ohm (2008, p. 1365) refers to as mythical “superusers”:

> We fear the Internet on several levels. First, we fear that the world is becoming less comprehensible to the average person. We fear that increasing technological complexity masks terrifying fragility: the world seems one cascading failure away from being unplugged, taking away all of the essential services we have migrated online in the past decade. Second, we fear malicious Superusers on the Internet for several reasons. We imagine the Internet teeming with all kinds of evildoers, from simple predators to ‘Supercriminal’ Superusers, such as organized crime figures, terrorists, and war fighters.

The sweep of the internet over essential, everyday infrastructure and its fragile, coded nature makes it an exceptional target for wreaking havoc by either disrupting it as such or, in the case of superusers, utilizing its instrumental abilities for malicious ends. When FBI Director Louis Freeh speaks of “some [criminal] organizations, particularly the large ones […] not only hiring their own software engineers, but [building] encrypted networks and global satellite communications to defeat our ability to access their criminal conversations with a court order” (Enforcement of Federal Drug Law, 1995), they are marshaling not only pre-existent mythological language about the sophistication and pernicious reach of organized crime, but a nascent set of mythological concepts regarding the uniquely threatening environs of the internet as a space where racialized others neutralize the rule of law. The synthesis of this relatively recent mythology with far older mythological figures of crime and disorder serves not only to reinforce the threatening atmosphere of the Internet but provides a new lens through which to magnify the purported threat of certain evergreen figures in the discourse of national security threats. Due to the constitution of these figures as racialized others, we see how a debate about cryptography,

perhaps seemingly far afield from the racial politics of the American carceral system and its logics, in fact represents a new frontier through which such logics may be re-articulated and emboldened.

Proposals for Deregulating Encryption: Mythologies of Foreign Hackers

In contrast to the police, intelligence, and congresspersons, who depict encryption as a threat to domestic social order because it harbors groups populated by racialized others and helps facilitate their deviant, criminal activity, corporations and digital rights advocates conceptualize encryption as crucial to ensuring America's economic hegemony and, by extension, protecting critical infrastructure and American industry from "unfriendly" foreign governments and their national corporations. In this understanding, the primary threat to the American people is not drug traffickers, gangs, or pedophiles, but the possibility of a globalized economy not headed by the U.S.

We can see these economic concerns clearly prioritized in the ways that industry representatives, digital rights advocates, and some policymakers conceptualize the relationship between encryption and crime. Although many acknowledge that encryption could potentially harbor deviant, criminal activity online, they insisted that the greater threat to U.S. national security actually comes from foreign countries and corporations—a new threat that has emerged due to globalization. Now that companies were outsourcing labor and subcontracting with foreign companies and international subsidiaries to take advantage of regional differences in the cost of labor and capital, they were more susceptible to foreign spying, corporate and industrial espionage, fraud, and hackers. Joseph Kretz of the FMC Corporation drew an explicit connection between globalization, U.S. economic hegemony, and the need to deregulate encryption:

> Competitive pressures are forcing businesses like FMC to work even more closely with suppliers, joint venture partners, and customers in an extended enterprise mode. This means that valuable proprietary designs, R&D data, and other strategic business information are constantly being transmitted and stored electronically around the world. This information must be protected if U.S. businesses are to remain competitive. (Encryption, 1997)

R. Patrick Watson of Eastman Kodak Company also raised the possibility that "foreign governments" could "monitor the legitimate activities of U.S. corporations and steal intellectual property for the benefit of national companies" (The Encryption Debate, 1997). The implication

of these statements is that the U.S. government's insistence on regulating encryption could prevent companies from dominating worldwide markets. Similarly, expert witnesses often argue that regulating encryption—specifically, imposing strict export controls which prevented U.S. companies from selling products in international markets if they contained encryption—would make U.S. companies less competitive, thus giving the upper hand to foreign firms. James Bidzos, president of RSA Data Security, Inc. suggested that:

> There is a product in South Africa that brags about being compatible with products in the U.S. The thing that I fear is that, once everybody starts to realize that they can buy a product outside the United States that is compatible with what they can get inside the United States, the next step might be for those products to become incompatible and for that overseas company to use encryption as a way to kind of get to the stop of the hill with this, and then use it as a way to throw us off by simply changing their product so it is no longer compatible. (S. 1726, 1996a)

The concern here is not simply with the competitiveness of American firms, but with their ability to set the technical standards early in the market's formation and thus solidify their power over economic production by controlling the underlying technical standards governing digital products. In this view, if American companies are not able to dominate digital markets (both online marketplaces and markets for digital products) early, they will permanently lose their ability to define the parameters and direction of these markets in the future, thus getting locked into an indefinite subordinate position relative to foreign countries.

The private sector consistently argues that economic espionage and intellectual property theft by foreign governments and companies not only impacts American businesses but damages American national security as well. For many of the speakers, American economic hegemony is a precondition for a healthy domestic democracy; if American companies lose out to foreign competitors, Americans will lose their jobs, be forced to depend on foreign products, and will therefore be subjected to the whims of foreign interests. Senator Patrick Leahy argues that "if we maintain current controls on encryption technology, then we lose control of the market. That means American companies, by the end of the year 2000, could lose $30 billion to $60 billion—the loss of almost 200,000 jobs at a time when, Mr. Chairman, we know that these high-tech jobs are the new jobs of the future" (S. 1726, 1996a). Rep. Smith reiterated this point a few years later: "E-commerce, the internet, all of that is becoming the leader, the driving force in our economy that is going to determine how strong our economy is, how high unemployment is,

whether or not my constituents or anybody else's constituents are able to get jobs. Us continuing to be the leaders in the IT economy is about the most important issue to people's economic security as anything out there" (U.S. Encryption Policy, 1999). Industry representatives, digital rights advocates, and policymakers who pushed for deregulating encryption habitually argued that encryption was crucial to ensuring American economic hegemony in the wake of globalization by protecting American people and companies from foreign countries. The speakers addressed (and in some instances, leveraged) widespread anxieties about future globalization, as well as lingering past anxieties of Cold War espionage, by depicting encryption as a technological fix that could protect the U.S. from foreign powers. This rhetoric is premised on a mythology of omission: most crime, including corporate espionage and other economic crimes, is not a function of foreign interference but occurs internally to corporations or by domestic competitors; this pattern of selectively emphasizing certain categories of crime and excluding others wholesale is, in many instances, the sine qua non of constructing myths regarding crime.

Accommodating Mythologies: A Compromise between the U.S. Government and IT Firms

Eventually, the Clinton administration and American IT firms reached a compromise. The government dropped its proposals to regulate encryption and agreed to lift export controls on encryption, allowing companies to sell their products with encryption abroad—and, by extension, expanding their user base and dominating global IT markets. However, we know from the Snowden disclosures that during this time, police and intelligence agencies brokered informal, backroom agreements with tech firms to ensure access to users' encrypted data and communications (e.g., Greenwald et al., 2013). We can see this incipient agreement in the 1990s congressional hearings, where congresspersons and IT company representatives argued that American corporations would work with law enforcement absent regulation—and in fact, that would be an ideal situation for the government, because they would be able to carve out a significant portion of the global IT market, ensuring that as many people as possible were using American products, thus granting police and intelligence agencies even greater surveillance capabilities. For example, James Bidzos of RSA Security suggested that American companies could be trusted to maintain their own methods for accessing their customers' encrypted communications: "The company can get into there in an emergency. Companies will want to do

that. Companies will deploy encryption when they have their own emergency access available to them and the government always has recourse with a court order to go in and demand information in that way." A year later, Ed Black—president of the Computer Communications Industry Association—reiterated this sentiment, stating that "the administration's approach is, in essence, top-down industrial policy. Key recovery should not, and we do not think can be, government-driven. It needs to be market-driven" (Encryption, 1997).

Speakers often argue that a market-driven approach to ensuring the government retains access to encrypted communications could benefit the state by ensuring more users trusted digital technologies. U.S. citizens, the argument went, do not trust their government but they do trust technology firms. If the latter are permitted to maintain their own access to their users' encrypted communications, users would be more likely to buy their products, thus ensuring the government had *more* access to communications. As James Lucier—sitting in for the president of Americans for Tax Reform, Grover Norquist—put it, "an encryption system that is not trusted by the marketplace is just not going to be used by anyone [...] Basically, in our view, key escrow, as it proposed right now, is an absolute showstopper for digital commerce" (S. 1726, 1996b). Similarly, Rep. Sonny Bono stated that:

> There's all this mystery about these agencies. That mystery has to be cleared up because it leaves a huge question mark in the minds of the public. I'm not prepared to give any agency more authority when I don't trust it. Frankly, I don't trust any of them—we're investigating the INS for releasing prisoners and other crimes. It's very nice to have this technical rhetoric we're having, but I would not be comfortable, nor would I even consider giving agencies more authority until they displaced more prudence in how they go about what they're supposed to do, as far as it's concerned with public safety. (Security and Freedom Through Encryption Act, 1996)

A year later, Rep. Sherman remarks that some people "might even trust Bill Gates with an extra copy of the key, but none of the people who have written me want to entrust the government with the key" (Encryption: Individual Right to Privacy, 1997). In essence, opponents of government proposals to ensure access to encrypted communications argue that people simply do not trust the government to appropriately decide when to access users' information, but they *do* trust tech firms with the same responsibility. American technology companies are seen by these actors much more trustworthy when it comes to deciding when they should, and should not, decrypt their customers' communications.

In fact, corporate representatives and some policymakers insist that American technology companies would voluntarily work with the U.S. government to ensure they could access user data in the absence of legislation demanding they do so. Roel Pieper, President and CEO of Tandem Computers, reminded Congress that "We, U.S. companies, must be able to compete," but assured them that "if we can compete, you can trust us that we will work with all the established security agencies around the world to then allow them to do their job with these technologies" (S. 1726, 1996b). The benefits of this informal, voluntary relationship would be severely diminished, however, if foreign companies came to dominate global technology markets. Roberta Katz of Netscape Communications Corporation states that:

> If America does lose this leadership, America's law enforcement and national security interests will be further compromised. While today American law enforcement can and actually does consult with American companies as the leaders in encryption technology, they will not be able to do this if, in fact, leadership in this area passes to foreign companies. We must keep in mind that the Internet is a global medium designed to facilitate cross-country communication. Surely, it is in America's interest for American companies to remain the encryption leaders, and this can only happen if American companies can meet the demand of the global marketplace. (Security and Freedom Through Encryption Act, 1996)

Later, in the same hearing, Katz reiterates that "if American companies lose their leadership in this area, as I said before, ultimately we harm our law enforcement and national security interests because the setting of the standards will move to foreign shores."

The argument here is that the private sector should be permitted to maintain their own encryption architecture while cooperating with law enforcement and intelligence to ensure they continue to have access to users' communications. Rep. Lofgren went so far as to call domestic companies "good Americans and patriots" who will "want to work with America in an appropriate fashion to do what they can" if "there is a threat to this country;" she later stated that Silicon Valley is full of "patriotic Americans who hate crime as much as you and I and can be counted on to act in appropriate ways" (Security and Freedom Through Encryption, 1997). In the same hearing, Rep. Goodlatte posed the following hypothetical question:

> Which is better from a national security standpoint: have U.S. companies creating the most up-to-the-minute encryption technology and applying it to software, or having foreign companies create that encryption technology? It seems to me we are better off in terms of our ability to work with the system to have it created in this country, rather than to have the Russians [...] It makes no sense to have Russians creating cryptography that we are going to use in this country. If there is going to be weak points in it, access to it, who is most likely to know about it, the U.S. government or the Russian government?

Similarly, Rep. Kennedy argues that "in this tech area, I think that we need to co-opt, if you will, American high technology because we are the leaders in the world. The fact of the matter is if we are going to intend to be the leaders in the world for our national security purposes, it seems to me we want to work with them and make sure that this stuff is going to be sold anyway, why not make sure they are on our side? If the product is being sold all over the world, why not make sure it is our product, domestic companies that have some allegiance and some interest in this country because they know about and appreciate the values of this great country of ours" (U.S. Encryption Policy, 1999). In short, proponents of deregulating encryption—by lifting export bans on digital products with encryption and by dropping federal proposals for a government-run key management infrastructure—position the technology industry as patriotic partners of American carceral institutions. Far from pushing back against the racist depictions of criminals which speakers mobilized to consolidate support for increased government surveillance, privacy advocates and industry representatives accepted the underlying logic of the government's proposals: that there is a massive crime problem that needs to be dealt with.

Encryption, Race, and Predatory Inclusion

At the outset, the Crypto Wars appear to have been fought between two sides: those pushing for increased government surveillance of all Americans and those fighting these proposals to protect individual privacy, with the state favouring the enrichment of its own power and the private sector loosely aligned with activists because of concerns about increased costs, decreased competitiveness, and ill-will among consumers generated by their participation in encryption regulation. This understanding is not only reductive in its consideration of the negotiations of the state and the private sector, but risks obviating the role of race as a constitutive force driving encryption policy by framing it in the generalized terms of its outcomes for the state and the private sector without considering the rhetorical tactics which are mobilized throughout. For

their part, state actors pathologically invoked mythological constructions of profoundly racialized criminal archetypes—especially gang members, terrorists, and sexual predators—to argue that the communicational reach of the internet, in concert with unfettered encryption, threatens to intensify violence, terror, and disruptions to social order. IT firms conjured images foreign governments employing spies and hackers who wish to destroy American infrastructure, all in service of bolstering their national corporations. In the private sector's account, these foreign others—depicted as a cabalistic set who refuse to follow the rules of global market capitalism by using state resources to give their firms an unfair competitive advantage—threatens to reverse the ostensible victory of capitalism in the Cold War by hamstringing American companies in the global market, resulting in the United States becoming economically dependent on other nations.

Both private sector and state actors advocated for their own interests during the Crypto Wars through constant recourse to mythological constructs, especially popular to the American imagination, concerning highly racialized and archetypal criminal figures. The new threat environment of the internet—itself a mythologized space founded on the contingency of insecurity and superpowered hackers, thereby understood to constitute an unprecedented threat environment—provides a second mythology enabling a mutually reinforcing mythic rhetoric wherein these archetypal criminal figures are further emboldened and empowered through the capabilities offered by the internet and unregulated encryption; conversely, these figures themselves provide an ideal population to rhetorically justify the need for extraordinary policing powers and strong regulation of encryption. Given the clear lineage of racialization in the establishment of the archetypes used most frequently and vociferously in these debates, the rhetoric of the Crypto Wars is, in no small part, a new permutation of pre-existent processes of racializing criminal mythologization.

We argue that the Crypto Wars, was a space for negotiating the conflicting logics of America's carceral institutions and an emergent network capitalism. Cottom (2020: 3) articulates a key reason why these two logics come into conflict: the internet's tendency towards expansion comes up against racism's desire to exclude, devalue, and stratify. Companies selling digital products become more profitable as their user base expands—hence why the industry tends towards

monopolization (Hindman, 2018). But racist, white supremacist American institutions have long been concerned with excluding people of color, whether from housing, finance, education, or politics. Cottom (2020: 3) argues that one way in which racial capitalism and platform capitalism are accommodated is through predatory inclusion: "the logic, organization, and technique of including marginalized consumer-citizens into ostensibly democratizing mobility schemes on extractive terms." The concept of predatory inclusion has been applied to understanding racial stratification in housing (Taylor, 2019) and debt (Seamster and Charon-Chénier, 2017). A key element of predatory inclusion is that it refers to the extractive, punitive inclusion of groups who were previously excluded from mechanisms of upward mobility that have historically been available to white people.

The Crypto Wars happened alongside the Clinton administration's transformation of technology policy into poverty policy (Greene 2021). Greene (2021, p. 31) points out a "core contradiction" in U.S. poverty policy, similar to that articulated by Cottom (2020): "On the one hand, the neoliberal state must offer promise: with the right skills, the global labor market becomes a space of unlimited potential where anyone can become an entrepreneur. On the other hand, the neoliberal state must threaten punishment: anyone who steps out of line will, at best, have their state support revoked or, at worst, be incarcerated." The Clinton administration resolved this contradiction by developing a new political common-sense Greene (2021, p. 5) calls the "access doctrine", or the belief that "the problem of poverty can be solved through the provision of new technologies and technical skills, giving those left out of the information economy the chance to catch up and compete." The salience of this common-sense has shaped our understanding of the relationship between the internet, the economy, and poverty to the point that institutions draw upon the access doctrine to secure legitimacy and resources, often "[turning] toward technology provision and skills-training programs because these garner economic and political support and make the problems they face more manageable" (Greene, 2021, p. 15)—a process Greene calls "bootstrapping." In some ways, bootstrapping resembles predatory inclusion in that both involve "the extension of long-withheld opportunities or resources for marginalized groups who seek social mobility, but on terms that disadvantage them in the long term and eventually reproduce inter-group inequality" (Greene, 2021, p. 169).

Can the Crypto Wars be conceived in similar terms? The regulatory debates of the early 1990s marked a critical juncture in which the U.S. federal government and American IT firms negotiated how to best include people of color in the burgeoning information economy. The American state, particularly police and intelligence agencies, wanted to prevent people of color from using strong encryption tools so that they could continue to police these communities; American IT firms, however, wanted to dominate global markets to prevent foreign countries from having control over international standards and infrastructure, while at the same time expanding their user base to include not only people of color in the U.S., but abroad as well. The eventual compromise these two sides reached—in which encryption was deregulated but law enforcement retained access to user data via informal, backdoor agreements—was crucial in setting the stage for the surveillance infrastructure in place today. In the late 1990s, the U.S. government dropped their proposals for encryption regulation while lifting export controls which prevented American companies from selling their products abroad. We have learned from the Snowden disclosures that shortly thereafter, many American companies entered informal, backdoor arrangements with tech firms to gain access to users' encrypted data (Ball et al., 2018; Gallagher and Moltke, 2018; Greenwald et al., 2013). Such agreements have been critical to the police and intelligence agencies' ability to conduct surveillance of people of color both inside and outside the United States.

Conclusion

National discourses on encryption regulation have remained remarkably stable over time. Catherine De Bolle and Cyrus R. Vance, Jr.—the executive director of Europol and the district attorney of New York County, respectively—recently published an article titled "The Last Refuge of the Criminal: Encrypted Smartphones." In it, they claim that "organized crime, terrorists, and child abusers are all drawn to devices and communication platforms that are designed to be technically impossible for law enforcement to law enforcement access." They go on to state that the Manhattan District Attorney was "hampered in accessing evidence in a recent child sex trafficking case, which should have provided important leads that could have saved additional trafficked children and found potential co-conspirators." The fact that these statements are indistinguishable from comments made 30 years ago suggests that there is an extremely effective and limited discursive condition at work where state arguments regarding encryption

are concerned. The axiomatic set of beliefs underwriting this discursive condition, i.e. the maintenance of immutable state dominance in all domains of law enforcement, leads to an essentially cyclical rhetoric which confronts new developments in encryption technology—and the radically shifting political contexts in which it is used—with uncannily identical tactics because of the fundamentally unchanging and relatively simplistic disposition regarding the absolute conservation of state juridical authority which constitutes its logic. The path of least resistance for this conservation of authority is the recurrent association of technologies which could fundamentally undercut state law enforcement capacities with the most well-established pantheon of criminal others at its disposal.

This presents an important opportunity for countersurveillance advocates and scholars to center race in their campaigns and analyses. The stability of national crypto discourses suggests that we are, in many ways, still grappling with the same questions we faced in the 1990s. As we continue to respond to police and intelligence agencies' calls for mandatory decryption capabilities, scholars and advocates could take this as an opportunity to question the underlying carceral and neoliberal logics motivating national technology policy. As vociferous calls for abolition echo from the streets, into our institutions, and into academia, we can no longer claim ignorance to the "unintended consequences" of our analyses (Parvin and Pollock, 2020). Rather, we need to seriously and thoroughly engage with how America's history of racism and white supremacy have, and continue to, structure technology policy as well as predominant critiques of it.

References

Aouragh, M., Gürses, S., Rocha, J., & Snelting, F. (2015). Let's First Get Things Done! On Division of Labour and Techno-political Practices of Delegation in Times of Crisis. *The Fibreculture Journal*, *26*, 208–235.

Ball, J., Borger, J., & Greenwald, G. (2018). Revealed: How the US and UK Spy Agencies Defeat Internet Privacy and Security. *The Guardian*. https://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security

Barthes, R., Lavers, A., & Barthes, R. (2006). *Mythologies*. Hill and Wang.

Browne, S. (2015). *Dark matters: On the surveillance of blackness*. Duke University Press.

Communications and Computer Surveillance, Privacy and Security, United States House of Representatives (1994).

Cottom, T. M. (2020). Where Platform Capitalism and Racial Capitalism Meet: The Sociology of Race and Racism in the Digital Society: *Sociology of Race and Ethnicity*, pp. 1-9.

De Bolle, C. & Vance C.R. (2021). The last refuge of the criminal: Encrypted smartphones. *Politico.* https://www.politico.eu/article/the-last-refuge-of-the-criminal-encrypted-smartphones-data-privacy

Dencik, L., Hintz, A., & Cable, J. (2016). Towards data justice? The ambiguity of anti-surveillance resistance in political activism. *Big Data & Society*, *3*(2).

Encryption, United States Senate (1997).

Encryption: Individual Right to Privacy vs. National Security, United States House of Representatives, 1 (1997).

Encryption, Key Recovery, and Privacy Protection in the Information Age, United States Senate (1997).

Encryption Security in a High Tech Era, United States House of Representatives (1999).

Enforcement of Federal Drug Laws: Strategies and Policies of the FBI and DEA, United States House of Representatives (1995).

Federal Bureau of Investigation, United States House of Representatives (2011).

Foucault, M. (2010). Truth and Power. In *The Foucault Reader* (pp. 51–75). Vintage Books.

Gallagher, R., & Moltke, H. (2018). The Wiretap Rooms: The NSA's Hidden Spy Hubs in Eight U.S. Cities. *The Intercept*. https://theintercept.com/2018/06/25/att-internet-nsa-spy-hubs/

Going Dark: Encryption, Technology, and the Balance Between Public Safety and Privacy, United States Senate (2015).

Going Dark: Lawful Electronic Surveillance in the Face of New Technologies, United States House of Representatives (2011).

Greene, D. (2021). *The promise of access: Technology, inequality, and the political economy of hope*. The MIT Press.

Greenwald, G., MacAskill, E., Poitras, L., Ackerman, S., & Rushe, D. (2013). Microsoft Handed the NSA Access to Encrypted Messages. *The Guardian*. https://www.theguardian.com/world/2013/jul/11/microsoft-nsa-collaboration-user-data

Gürses, S., Kundnani, A., & Van Hoboken, J. (2016). Crypto and empire: The contradictions of counter-surveillance advocacy. *Media, Culture & Society*, *38*(4), 576–590.

Hindman, M. (2018). *The Internet Trap: How the Digital Economy Builds Monopolies and Undermines Democracy*. Princeton University Press.

Kappeler, V. E., & Potter, G. W. (2018). *The mythology of crime and criminal justice* (Fifth edition). Waveland Press.

Kaye, D. (2015). *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression* (pp. 1–21). United Nations.

Mbembe, A. (2019). *Necropolitics* (S. Corcoran, Trans.). Duke University Press.

McLaughlin, J. (2015). Exclusive: Edward Snowden Explains Why Apple Should Continue to Fight the Government on Encryption. *The Intercept*. https://theintercept.com/2015/07/31/exclusive-edward-snowden-says-obama-administrations-war-encryption-just-doesnt-make-sense/

Ohm, P. (2008). The Myth of the Superuser: Fear, Risk, and Harm Online. *UC Davis Law Review*, *41*(4), 1327–1402.

Parvin, N., & Pollock, A. (2020). Unintended by Design: On the Political Uses of "Unintended Consequences." *Engaging Science, Technology, and Society*, *6*, 320-327.

Privacy in the Digital Age: Encryption and Mandatory Access, United States Senate (1998).

Rexhepi, P. (2016). Liberal Luxury: Decentering Snowden, Surveillance and Privilege. *Big Data & Society*, *2*, 1–3.

S. 1726, Promotion of Commerce Online in the Digital Era Act of 1996, or "PRO-CODE" Act, United States Senate (1996).

S. 1726, The Promotion of Commerce Online in the Digital Era Act of 1996, or "PRO-CODE" Act, United States Senate (1996).

Seamster, L., & Charron-Chénier, R. (2017). Predatory Inclusion and Education Debt: Rethinking the Racial Wealth Gap. *Social Currents*, *4*(3), 199–207.

Security and Freedom through Encryption (SAFE) Act, United States House of Representatives (1996).

Stevens, A., & Allen-Robertson, J. (2021). Encrypting human rights: The intertwining of resistant voices in the UK state surveillance debate. *Big Data & Society*, *8*(1).

Taylor, K.-Y. (2019). *Race for profit: How banks and the real estate industry undermined black homeownership*. The University of North Carolina Press.

Telecommunications Network Security, United States House of Representatives (1993).

Terrorism Gone Viral: The Attack in Garland, Texas, and Beyond, United States House of Representatives (2015).

The Administration's Clipper Chip Key Escrow Encryption Program, United States Senate (1994).

The Encryption Debate: Criminals, Terrorists, and the Security Needs of Business and Industry, United States Senate (1997).

The Security and Freedom Through Encryption (SAFE) Act, United States House of Representatives (1997).

U.S. Encryption Policy, United States House of Representatives (1999).

West, S. M. (2018). Cryptographic Imaginaries and the Networked Public. *Internet Policy Review*, *7*(2), 1–16.

West, S. M. (2021). Survival of the cryptic: Tracing technological imaginaries across ideologies, infrastructures, and community practices. *New Media & Society*, pp. 1-21.