The Golden Age of Racial Surveillance

Michael Kwet

We are living in times of deep turmoil and rapid change. Over the past few decades, inequality has increased within and between countries. Simultaneously, new developments in digital technology have spread throughout the world, reconfiguring power relations and the rhythms of everyday life. Transnational technology corporations and powerful nation states have been the primary beneficiaries of the digital revolution, and their domination of digital technology concentrates power and wealth into their hands. The United States dominates the global tech economy, an evolution of American empire. Computers, wired together across the Internet, have drastically expanded the capacity to spy on and assess individuals, groups, and populations.

Surveillance has long been used a tool for the oppression and control of those being watched. As Noam Chomsky puts it, surveillance technology can be used "for making money, and you can use it for controlling people's attitudes and beliefs, directing them toward what you want them to do." Throughout modern history, surveillance has been developed and used by racially dominant groups to direct them toward "what they want them to do," most often for the purpose of exploitation and profit.

This volume chronicles how surveillance (re)produces racial inequality. Across sixteen chapters, it takes a deep dive into historical and contemporary developments, crisscrossing time and space to develop a global picture of race and surveillance.

Jason Hickel, The Divide: Global Inequality from Conquest to Free Markets (New York: W. W. Norton & Company, Inc., 2017).

Michael Kwet, "Digital Colonialism: US Empire and the New Imperialism in the Global South," Race & Class 60, no. 4 (2019); Michael Kwet, "Digital Colonialism: The Evolution of American Empire," ROAR, March 3, 2021, https://roarmag.org/essays/digital-colonialism-the-evolution-of-american-empire.

Noam Chomsky, Global Discontents: Conversations on the Rising Threats to Democracy (New York: Metropolitan Books, 2017), 2.

It can be read by general and scholarly audiences, and is of critical value to anyone looking to grapple with the racialized surveillance state expanding across the world.

The use of surveillance for racial control is, of course, nothing new. For example, surveillance infrastructure in America was developed through the practice of slavery and indentured servitude. As Christian Parenti remarks, white slave holders "were forced to develop not just methods of terror but also a haphazard system of identification and surveillance." Written slave passes were used in conjunction with organized slave patrols and wanted posters for runaways to police the mobility of African bodies. Skin branding with marks of slave owners were also used to catalog and keep tabs on slaves. In New York City, lantern laws required people of color to carry candle lanterns in the dark. White people were deputized to police black persons traveling in the dark without a lantern, and those caught without one could be punished with lashings, to be determined by the slave owner. In the domain of labor, white slaveholders recorded the activity of slave farmers and analyzed the data to predict and alter their work routines to maximize production.

While these histories expose important methods of control and exploitation within the United States, racialized surveillance extends well beyond US borders.

As Amber Sinha and Shruti Trikanand show in this volume, in India, the British targeted caste and tribes for alleged "criminality" as a means to classify, discipline, and punish "criminal tribes" – that is, those deemed genetically prone to crime. Tribes could be relocated by the British colonizers or placed in a "reformatory settlement." Passes were issued to police movements, and local authorities were empowered to surveil tribe members and inspect their places of residence. Law enforcement agencies maintained "historical sheets" that put people accused of crimes on police surveillance lists.

In Victorian Britain, Toni Weller demonstrates how women were deemed categorically different than men – almost as if they were a separate race – and women themselves became platforms for surveillance. British authorities drew upon pseudoscientific theories of evolution to impose control and order over women's bodies and minds.

In South Africa, Michael Kwet details how surveillance goes hand-in-hand with racial domination in South Africa. Colonizers used pass systems, skin branding, fingerprinting, and eventually computer systems to classify, monitor, and police the bodies and labor of Africans and other people of color. In each phase of South African history, US authorities increased their support of surveillance by white supremacist authorities in the country. Today, the United States is directly

⁴ Christian Parenti, The Soft Cage: Surveillance in America from Slave Passes to the War on Terror (New York: Basic Books, 2003), 14.

⁵ Simone Browne, Dark Matters: On the Surveillance of Blackness (Athens, GA: Duke University Press, 2015), 31–88.

⁶ Caitlin Rosenthal, Accounting for Slavery: Masters and Management (Cambridge, MA: Harvard University Press, 2018).

administering mass surveillance in South Africa, this time through the process of digital colonialism.

In Brazil, Claudio Altenhain et al. trace the history of race and surveillance, connecting today's surveillance regimes in urban spaces to early forms of surveillance arrangements used to segregate and exploit bodies according to skin color. In Israel and Palestine, Yasmeen Abu-Laban and Abigail B. Bakan show how authorities are using surveillance against those calling for boycott, divestment, and sanctions (BDS) against Israel. And in Xinjiang, Myunghee Lee and Emir Yazici detail the Chinese Communist Party's (CCP) extreme repression of the Uyghur population. A vast array of dystopian technologies is being used en masse to surveil Uyghurs, who have been subject to indoctrination and brutal treatment by CCP authorities.

Surveillance technologies often travel across borders. In South Africa and India, fingerprinting technologies were imposed by the British, and experiments in using them to police dark-skinned bodies flowed across the colonies. In Chapter 3, Alfred McCov illustrates how surveillance technologies were first used by American imperialists to conquer the Philippines, but soon thereafter migrated back home. McCoy traces the emergence of the modern US surveillance state to "America's first information revolution" used to colonize the Philippines at the turn of the nineteenth century. Thomas Edison's quadroplex telegraph (1874), Philo Remington's commercial typewriter (1874), and Alexander Graham Bell's telephone (1876) "allowed the transmission and recording of textual data in unprecedented quantities at unequaled speed with unsurpassed accuracy." Melvil Dewey's Dewey Decimal System enabled efficient encoding and the rapid retrieval of information, and Herman Hollerith's punchcard system sped up population registers for census records.⁸ Meanwhile, John Gamewell's corporation wired up police telegraph/ telephone call-box systems. In short time, hundreds of US municipal security networks were sending 41 million messages per year. Biometric analytics (such as fingerprinting and Alphonse Bertillon's photographic identification) and new statistical methods (such as statistical regression) were invented, which helped make sense of the surveillance data.

The policing panopticon formed abroad would soon come home to the United States. During World War I, the "father of American military intelligence," Ralph Van Deman, designed the United States' first internal security agency as head of the US Military Intelligence Section. In collaboration with the Bureau of Investigation (FBI), McCoy observes, Van Deman presided over a counterintelligence auxiliary, the American Protective League, with 350,000 civilian operatives who amassed over

Alfred McCoy, Policing America's Empire: The United States, the Philippines, and the Rise of the Surveillance State (Madison, WI: The University of Wisconsin Press), 21–27; Alfred McCoy, "Policing the Imperial Periphery: The Philippine-American War and the Origins of U.S. Global Surveillance," Surveillance & Society 13, no. 1 (2015): 4–26, 9–10.

⁸ Hollerith went on to found IBM and the technology was used by South Africa's apartheid government decades later.

Michael Kwet

4

a million pages of surveillance reports on German Americans in just fourteen months. New intelligence institutions rapidly expanded to suppress strikes and the socialist left in the United States. The Lusk Raids in New York City investigated the "seditious activities" of "radicals" and "radical organizations" – including the Rand School of Social Science, which aimed at socialist education. J. Edgar Hoover's Palmer Raids targeted anarchists and other socialists for activity such as labor strikes and political assassinations. Following his retirement from the army in 1929, Van Deman spent almost twenty-five years amassing detailed files on 250,000 suspected subversives.

A second wave of surveillance commenced around World War II. The FBI and California Committee on Un-American Activities pursued a new "red scare" against the US Communist Party and its alleged allies in Hollywood. When Van Deman died in 1952, his archive was secured by the US Army Counter Intelligence Corps, who used it against "communist" adversaries for the next two decades. Van Deman's surveillance tactics were also used by the FBI for wiretapping, illegal break-ins, and mail intercepts. Domestic surveillance targets included US politicians as well as academics, cultural icons, and members of the general public.

Today, a second information revolution, once again developed in the United States, brings together advances in computing, storage, processing, sensing, statistics (including so-called artificial intelligence), network connectivity, and data transmission. As with the first information revolution, authorities are making use of the new tech for social control, military, and policing purposes.

During the 2000s, a succession of US whistleblowers revealed that the US government formed a surveillance dragnet designed to mop up the world's communications. In 2013, Edward Snowden leaked hundreds of thousands of files from the National Security Agency (NSA) to journalists, who exposed much of the NSA's mass surveillance programs in detail. Through the Snowden leaks, we learned how the NSA conducts dragnet and targeted surveillance all across the world. The Middle East is a primary target. As part of the so-called "War on Terror," Muslims are spied on with no legal or practical recourse. This includes mass dragnet surveillance – for instance, Wikileaks revealed that the metadata and content of phone calls in the Bahamas and Afghanistan were recorded by the NSA, via its MYSTIC program, and held for thirty days for playback on demand – as well as targeted surveillance via programs like the National Counterterrorism Center's database of

9 For skeptical views of artificial intelligence as "intelligence" and the topic of whether machines can think, see Noam Chomsky, New Horizons in the Study of Language and Mind (Cambridge, MA: Cambridge University Press, 2000), 44–45. For other skeptical takes on AI and its adverse impact on race relations and other social ills, see Yarden Katz, "Manufacturing an Artificial Intelligence Revolution" (SSRN, 2017), https://papers.csm.com/sol3/papers.cfm? abstract_id=3078224; Gary Smith, The AI Delusion (Oxford University Press, 2018); Meredith Broussard, Artificial Unintelligence: How Computers Misunderstand the World (Cambridge, MA: 2018); Yarden Katz, Artificial Whiteness: Politics and Ideology in Artificial Intelligence (New York: Columbia University Press, 2020).

terrorism suspects. Other surveillance projects revealed that the United States and its allies, such as the United Kingdom's Government Communications Headquarters (GCHQ), have spied on diplomats conducting trade negotiations, as well as nongovernmental organizations, activists, and corporations, in countries like South Africa and Brazil. The use of mass and targeted surveillance by the world's most powerful governments is in service of empire. People of color are disproportionately in the crosshairs.¹⁰

In cities, a similar dynamic is at play. The use of sensors and the means to make sense of surveillance data has increased exponentially over the past two decades. Closed-circuit television (CCTV) cameras are central to an emerging surveillance industrial complex. Where CCTVs once provided blurry images recorded to tape on a single plot of land – making it impossible to track individuals across a wide geography – city authorities now operate advanced CCTV networks that unite thousands of high-resolution cameras into a single network. Thanks to advances in computing, we now have "smart" cameras that can identify faces, objects, and behaviors so that authorities can record, index, and make sense of the data filmed by thousands of cameras across a wide area. Through a "plug-in surveillance" model, businesses and residents are increasingly adding their own cameras to police networks so that they may access more footage of public spaces.¹¹ Drones are also spying from up high, allowing authorities to monitor what goes on in the city down below. Police can now watch over the entire city from centralized command-and-control centers. In many cities, outside life is becoming a filmed experience.¹²

Centralized city surveillance is expanding in sophistication and use cases. In the United States, fusion centers – surveillance centers that pool information from multiple sources into one location for information sharing between agencies – proliferated in the wake of the 9/11 attacks. The model seems to have served as a template in other countries, such as South Africa, where the Free State province was reported to be building its own fusion center.¹³

In parallel, real-time crime centers (RTCC) for police emerged with the expansion of technology for used monitoring and investigations. ¹⁴ RTCCs pool data

- See Glenn Greenwald, No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State (New York: Metropolitan Books, 2014); Jennifer Stitsa Granick, American Spies: Modern Surveillance, Why You Should Care, and What to Do About It (Cambridge University Press); Edward Snowden, Permanent Record (New York: Metropolitan Books, 2019).
- Michael Kwet, "The Rise of Smart Camera Networks, and Why We Should Ban Them," The Intercept, January 27, 2020, https://theintercept.com/2020/01/27/surveillance-cctv-smart-camera-networks
- ¹² Arthur Holland Michel, Eyes in the Sky: The Secret Rise of Gorgon Stare and How It Will Watch Us All (New York: Harcourt Publishing Company, 2019).
- ¹³ Michael Kwet, "Apartheid in the Shadows: The USA, IBM and South Africa's Digital Police State," Counterpunch, May 3, 2017, www.counterpunch.org/2017/05/03/apartheid-in-the-shadows-the-usa-ibm-and-south-africas-digital-police-state.
- ¹⁴ There is little available in the public record about real-time crime centers. For details on their origins and development, see Michael Kwet and Paul Prinsloo, "The 'Smart' Classroom:

6

from surveillance sensors and records into one pot for storage, analysis, and real-time information sharing with boots on the ground. Corporations provide the software, infrastructure, and services needed to manage the surveillance databases ingested by these twenty-first-century surveillance centers. In New York City, Microsoft partnered with the New York Police Department (NYPD) to build a Domain Awareness System (DAS) it calls Microsoft Aware – a software platform that pools surveillance, records, and other data for real-time and long-term city surveillance. Surveillance cameras, acoustic ShotSpotter sensors, chemical sensors, and license plate readers pull information from the streets into the system, which makes use of facial recognition and license plate readers. Tens of databases were pooled into the center for data analytics, including predictive policing used for criminal investigations. As part of the deal, the NYPD gets a 30 percent cut of the revenue from sales of the system to other Microsoft Aware customers. Soon after the system was unveiled in 2012, Microsoft sold its Aware solution to Atlanta; Washington DC; Singapore; Bulgaria; and São Paulo, Brazil. 15

Microsoft has also adopted its Aware solution for prisons – currently on offer in the UK – in a move to capture the emerging market to "upgrade" and digitize the carceral pipeline using twenty-first-century technologies. Through its Public Safety and Justice division, Microsoft works with third-party vendors supplying surveillance technology to police, jails and prisons (including for juveniles), immigration authorities, the courts, services for pretrial and probation, and social media surveillance. As several chapters highlight in this volume, with these systems, people of color are targeted, sentenced, and imprisoned at rates greater than the white population. Researchers have shown time and again that the deployment of solutions like facial recognition and predictive policing have racially biased and adverse effects on people of color while failing to provide the outcomes advertised by the vendors selling them.

Police and intelligence agencies are also using special software to monitor and target persons of interest. Some authorities use cell site simulators to spy on people

A New Frontier in the Age of the Smart University," *Teaching in Higher Education* 25, no. 4 (2020): 510–526. For a general history of police surveillance technology in the United States into the digital era, see Brian Jefferson, *Digitize and Punish: Racial Criminalization in the Digital Age* (University of Minnesota Press, 2020).

¹⁵ For an overview of Microsoft's relationship to police, see Michael Kwet, "The Microsoft Police State: Mass Surveillance, Facial Recognition, and the Azure Cloud," *The Intercept*, July 14, 2020, https://theintercept.com/2020/07/14/microsoft-police-state-mass-surveillance-facial-recognition; Chris Gelardi, "Inside D.C. Police's Sprawling Network of Surveillance," *The Intercept*, June 18, 2022, https://theintercept.com/2022/06/18/dc-police-surveillance-network-protests.

¹⁶ Ibid.; Michael Kwet, "Microsoft's Iron Cage: Prison Surveillance and e-Carceration," Al Jazeera, www.aljazeera.com/features/2020/12/21/microsofts-iron-cage-prison-surveillance-and-e-carceral-state; Michael Kwet, "ShadowDragon: Inside the Social Media Surveillance Software That Can Watch Your Every Move," The Intercept, September 21, 2021, https://theintercept.com/2021/09/21/surveillance-social-media-police-microsoft-shadowdragon-kaseware.

in a broad area.¹⁷ These devices mimic cell phone towers and trick phones near them to transmit their location and identifying information. In some versions, the device can clone a target's phone and make/receive calls and text messages that will appear as if they are coming from the target's number; capture metadata about calls such as who is being called and for how long; capture text messages; listen to and record audio from the target's handset; and intercept data usage, such as websites visited.¹⁸ Civil rights and liberties advocates have raised concerns that cell site simulators are being used in black and brown neighborhoods to target people of color and activists.¹⁹

Carceral authorities and intelligence agencies also target phones with specialized software used to hack into devices and exfiltrate information. The Israeli firm NSO Group produces the notorious hacking software, Pegasus, which enables almost unlimited remote monitor of target cellphones. In 2018, the Israeli news media outlet *Haaretz* published an in-depth exposé revealing that NSO Group, together with other Israeli firms, sell cybersurveillance software to scores of dictatorships and authoritarian regimes that use their software to "locate and detain human rights activists, persecute members of the LGBT community, silence citizens who were critical of their government and even to fabricate cases of blasphemy against Islam." The issue reemerged in 2021 when a massive data leak suggested repressive regimes have been using NSO Group spyware to target journalists, activists, heads of state, and other persons of interest. ²¹

Some of these software solutions are used to monitor social media. For example, Israeli firm Verint's product-line clients in Azerbaijan inquired about using its software to "check sexual inclinations" of Facebook users. Years later, a 2017 report

- For an explanation of how cell site simulators work, see Electronic Frontier Foundation, "Street-Level Surveillance: Cell-Site Simulators/IMSI Catchers," (n.d.), www.eff.org/pages/cell-sitesimulatorsimsi-catchers.
- ¹⁸ Shaun Swingler, "Meet the Grabber: How Government and Criminals Can Spy on You (and How to Protect Yourself)," *Daily Maverick*, September 1, 2016, www.dailymaverick.co.za/ article/2016-09-01-meet-the-grabber-how-government-and-criminals-can-spy-on-you-and-how-to-protect-yourself.
- 19 See Harvey Gee, "Stingray Cell-Site Simulator Surveillance and the Fourth Amendment in the Twenty-First Century: A Review of The Fourth Amendment in the Twenty-First Century: A Review of The Fourth Amendment in an Age of Surveillance, and Unwarranted Amendment in an Age of Surveillance, and Unwarranted," St. John's Law Review 93, no. 2 (2019): 325–364; Brian Barrett, "The Baltimore PD's Race Bias Extends to High-Tech Spying, Too," Wired, August 16, 2016, www.wired.com/2016/08/baltimore-pds-race-bias-extends-high-tech-spying.
- Hagar Shezaf and Jonathan Jacobson, "Revealed: Israel's Cyber-spy Industry Helps World Dictators Hunt Dissidents and Gays," *Haaretz*, October 20, 2018, www.haaretz.com/israelnews/.premium.MAGAZINE-israel-s-cyber-spy-industry-aids-dictators-hunt-dissidents-and-gays-1.6573027.
- Amnesty International, "Massive Data Leak Reveals Israeli NSO Group's Spyware Used to Target Activists, Journalists, and Political Leaders Globally," July 18, 2021, www.amnesty.org/ en/latest/press-release/2021/07/the-pegasus-project.

Michael Kwet

8

by Human Rights Watch detailed the arrest and torture of persons presumed to be gay, bisexual, or transgender. In Indonesia, Verint was used to create a database of LGBT persons and religious minorities.²²

Social media software has also been used to target Black Lives Matter protesters and journalists in the United States. Dataminr, *The Intercept* reported in 2020, "relayed tweets and other social media content about the George Floyd and Black Lives Matter protests directly to police, apparently across the country." Another product, ShadowDragon, is being used by police in the United States and elsehwere, which has raised concerns by civil rights and liberties organizations, who are calling to ban it. ²⁴

The line between commercial surveillance and police surveillance has increasingly blurred during the digital era. NSA surveillance is largely reliant upon the cooperation of tech corporations, who provide access to communications streams (such as data transmitted over internet cables) and the databases they store in cloud server farms. For instance, through NSA's PRISM program, the NSA collects stored internet communications from Microsoft, Yahoo, Google, Facebook, PalTalk, YouTube, Skype, AOL, and Apple. Using XKEYSCORE, the NSA and its allies in Australia, Canada, New Zealand, Britain, Japan, and Germany can search and analyze global internet content. Snowden said that XKEYSCORE is a "one-stop shop for access to the NSA's information" that allows users to search for emails, track website traffic and laptops, and more.²⁵

Indeed, a wide variety of government agencies are piggybacking on Big Tech's commercial surveillance. In the United States, police are serving tech corporations warrants for search history data, speakers, wearables, and smart home technologies like IoT devices.²⁶ The Internal Revenue Service, FBI, Department of Homeland

- ²² Human Rights Watch, "Azerbaijan: Anti-Gay Crackdown: Gay Men, Transgender Women Tortured to Extort Money, Intelligence," October 3, 2017, www.hrw.org/news/2017/10/03/azer baijan-anti-gay-crackdown.
- ²³ Sam Biddle, "Police Surveilled George Floyd Protests With Help From Twitter-Affiliated Startup Dataminr," *The Intercept*, July 9, 2020, https://theintercept.com/2020/07/09/twitter-dataminr-police-spy-surveillance-black-lives-matter-protests.
- ²⁴ Kwet, "ShadowDragon."
- NDR.de, "Snowden-Interview: Transcript," January 26, 2014, https://web.archive.org/web/ 20140128224439/http://www.ndr.de/ratgeber/netzwelt/snowden277_page-3.html.
- See, among others, Sidney Fussell, "How Your Digital Trails Wind Up in the Police's Hands," Wired, December 28, 2020, www.wired.com/story/your-digital-trails-polices-hands; Frank Green, "Are 'Geofence' Warrants a Legitimate Investigative Tool or an Unconstitutional 'Digital Dragnet'? Chesterfield Robbery Case Raises Privacy Questions," Richmond Times-Dispatch, June 24, 2021, https://richmond.com/news/local/crime-and-courts/are-geofence-war rants-a-legitimate-investigative-tool-or-an-unconstitutional-digital-dragnet-chesterfield-robbery-case/article_bf3do1a7-d9ec-5a2c-bfe2-298630e69ea7.html; Albert Fox Cahn and Justin Sherman, "Your 'Smart Home' Is Watching and Possibly Sharing Your Data with the Police," The Guardian, April 5, 2021, www.theguardian.com/commentisfree/2021/apr/o5/techpolice-surveillance-smart-home-devices; Lorenzo Franceschi-Bicchierai, "Here's How Police Request Data from WhatsApp and Facebook," VICE News/Motherboard, www.vice.com/en/

Security, and Department of Defense have all purchased cell phone data.²⁷ In 2020, a data analytics firm, Mobilewalla, released a report predicting the place of residence, race, age, and gender of 17,000 George Floyd protesters in four US cities. While Mobilewalla pledged not to sell the protest data to clients or policing agencies, it demonstrated the power of private firms to monitor protesters and profile them according to their identities, thereby exposing the public to racial profiling with the potential to undermine freedom of assembly.²⁸ And now that *Roe v. Wade* has been overturned, women seeking abortions in US states banning the practice fear their data will fall into the hands of the police and judicial authorities.²⁹ Women of color, who in some states have higher rates of abortion than white women and often lack access to and effective use of contraception, would be disproportionately affected.³⁰

Commercial surveillance itself also (re)produces racial inequality. For example, in 2016, *Business Insider* reported that Facebook let advertisers exclude users by race using a tool called Ethnic Affinities. The feature used data points about users to categorize them into four categories: non-multicultural (ostensibly white), African American, Asian American, and Hispanic. *Ars Technica* demonstrated that different users were shown different versions of the trailer for the movie, *Straight Outta Compton*.³¹ The "general population" (non-African American, non-Hispanic) was presumed unfamiliar with the music group, N.W.A., on which the film is based, and so was given a trailer which provided context. The trailer given to the African

- article/k7q94v/heres-how-police-request-data-from-whatsapp-and-facebook; Zack Whittaker, "This Is How Police Request Customer Data from Amazon," *Tech Crunch*, September 27, 2020, https://techcrunch.com/2020/09/27/this-is-how-police-request-customer-data-from-amazon; Laura Dobberstein, "Microsoft Tells US Lawmakers Cloud Has Changed the Game on Data Privacy, Gets 10 Info Demands *a Day* from Cops," *The Register*, July 2, 2021, www.theregister.com/2021/07/02/us_government_cloud.
- ²⁷ Joseph Cox, "How the U.S. Military Buys Location Data from Ordinary Apps," VICE News/ Motherboard, November 16, 2020, www.vice.com/en/article/jgqm5x/us-military-location-dataxmode-locate-x; Albert Fox Cahn and Jake Laperruque, "Putting a Price on Privacy: Ending Police Data Purchases," The Hill, May 6, 2021, https://thehill.com/opinion/technology/552105putting-a-price-on-privacy-ending-police-data-purchases; Laura Hecht-Felella, "Federal Agencies Are Secretly Buying Consumer Data," Brennan Center for Justice, April 16, 2021, www.brennancenter.org/our-work/analysis-opinion/federal-agencies-are-secretly-buying-con sumer-data.
- ²⁸ Caroline Haskins, "Almost 17,000 Protesters Had No Idea a Tech Company Was Tracing Their Location," *Buzzfeed News*, June 25, 2020, www.buzzfeednews.com/article/carolinehaskins1/ protests-tech-company-spying.
- ²⁹ Sara Morrison, "What Police Could Find Out about Your Illegal Abortion," Vox, June 24, 2022, www.vox.com/recode/23059057/privacy-abortion-phone-data-roe.
- 3º Anne Branigin and Samantha Chery, "Women of color Will Be Most Impacted by the End of Roe, Experts Say," The Washington Post, June 24, 2022, www.washingtonpost.com/nation/2022/ 06/24/women-of-color-end-of-roe.
- ³¹ Analee Newitz, "Facebook's Ad Platform Now Guesses at Your Race Based on Your Behavior," Ars Technica, March 18, 2016, https://arstechnica.com/information-technology/2016/03/face books-ad-platform-now-guesses-at-your-race-based-on-your-behavior.

10

Americans Affinity Group was different: it assumed baseline familiarity with N.W.A. While technically any person could be categorized in any Ethnic Affinity group – the algorithm assigned categories based on data points, as Facebook users do not declare their race to the network – the assumption is that most people placed into specific Affinity Groups do indeed fit the corresponding racial category. This was the purpose of the tool, after all.³²

By October 2016, *ProPublica* revealed that racial customization via Ethnic Affinities can be used to discriminate against racial groups.³³ Its journalists ordered housing advertisements on Facebook and targeted them to users who were house hunting, excluding African-American, Asian-American, and Hispanic Affinity Groups. Facebook approved the ads, even though discrimination in housing advertisements violates the Civil Rights Act of 1994. In response, Facebook began building new tools to disable the use of ethnic affinity marketing for certain types of ads and it removed "thousands of categories from exclusion targeting related to potentially sensitive personal attributes, such as race, ethnicity, sexual orientation and religion" – including the "multicultural affinity" category.³⁴ While Facebook has declared it reined in the ability for racial targeting, an investigation at *The Markup* found that advertisers could still use the platform to target users on the basis of race.³⁵ Facing public pressure, Facebook finally announced that it will end advertising based on politics, race, and other "sensitive" topics.³⁶

Schools are another site of mass surveillance where the line between business and the state is blurred. Visual surveillance manufacturers are pushing cameras into schools on the premise that more cameras can make campus grounds safer and more efficient via smart technologies.³⁷ Big data surveillance is also becoming part of the educational landscape. Many students and teachers are now being forced to use surveillance-driven big data tools for the purpose of "data analytics" and

Nathan McAlone, "Why 'Straight Outta Compton' had different Facebook Trailers for People of Different Races," *Business Insider*, March 16, 2016, www.businessinsider.com/why-straight-outta-compton-had-different-trailers-for-people-of-different-races.

³³ Julia Angwin and Terry Paris Jr., "Facebook Lets Advertisers Exclude Users by Race," ProPublica, October 28, 2016, www.propublica.org/article/facebook-lets-advertisers-exclude-users-by-race.

³⁴ Erin Egan, "Improving Enforcement and Promoting Diversity: Updates to Ethnic Affinity Marketing," Facebook, November 11, 2016, https://about.fb.com/news/2016/11/updates-to-ethnic-affinity-marketing; Facebook Business, "Reviewing Targeting to Ensure Advertising is Safe and Civil," April 24, 2018, www.facebook.com/business/news/reviewing-targeting-to-ensure-advertising-is-safe-and-civil; Facebook Business, "Simplifying Targeting Categories," August 11, 2020, www.facebook.com/business/news/update-to-facebook-ads-targeting-categories.

³⁵ Jon Keegan, "Facebook Got Rid of Racial Ad Categories. Or Did It?" The Markup, July 9, 2021, https://themarkup.org/citizen-browser/2021/07/09/facebook-got-rid-of-racial-ad-categories-or-didit

³⁶ Shannon Bond, "Facebook Scraps Ad Targeting Based on politics, Race and Other 'Sensitive' Topics," NPR, November 9, 2021, www.npr.org/2021/11/09/1054021911/facebook-scraps-ad-targeting-politics-race-sensitive-topics.

³⁷ Kwet and Prinsloo, "The 'Smart' Classroom."

management.³⁸ Two chapters will take up the presence of police and surveillance in schools, including the adverse impact it often has on children of color.

Other big data practices have been criticized for racial discrimination. In 2012, a group of researchers found that the six facial algorithms they tested have lower accuracy for black than white subjects.³⁹ In 2018, the issue exploded internationally when a team of researchers found that facial recognition algorithms deployed by IBM, Microsoft, and Face++ were less accurate for black subjects than for white subjects.⁴⁰ By this time, there was growing public concern about the adverse effects of algorithmic bias on marginalized groups.⁴¹

Despite the dangers of algorithmic discrimination and the disparate impact of surveillance on vulnerable populations, biometric profiling is on the rise. Several chapters detail how biometric identification is derived from racist Western policing practices. India is pioneering a new wave of biometric identification through its controversial Aadhaar identification system. As Sinha and Trikanad explain, what started off as a registration system for citizen identification grew into a "cradle to grave" identity system used across a multitude of government agencies that already do, or intend to, keep track of health, employment, income, religion, caste, and other economic and demographic information; issue things like arms licenses and ration cards; collect information about crime, education, employment, taxes, marital status, religion; and more. The Aadhaar identification system assigned to residents in India constitutes an infrastructure for mass surveillance.

The US military has imposed new biometric technologies on people living in the Middle East. In Iraq, the Defense Department amassed a record of iris scans, fingerprints, DNA, and other biometrics in a database of 3 million Iraqis. In Afghanistan, the US military also constructed a massive biometric database of Afghans and used giant balloons equipped with sophisticated cameras and sensors to spy on the population below. Palantir Technologies was contracted to deploy

- 38 See Michael Kwet, "Operation Phakisa Education: Why a Secret?" First Monday, 22, no. 12 (2017), https://firstmonday.org/ojs/index.php/fm/article/view/8054; Cathy O'Neil, Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Our Democracy (New York: Broadway Books, 2017), 50–67; Roxana Marachi, "The Case of Canvas: Longitudinal Datafication through Learning Management Systems," Teaching in Higher Education 25, no. 4 (2020): 418–434.
- ³⁹ Brendan F. Klare, Mark J. Burge, Joshua C. Klontz, Richard W. Vorder Bruegge, and Anil K. Jain, "Face Recognition Performance: Role of Demographic Information," *IEEE* (2012), http://openbiometrics.org/publications/klare2012demographics.pdf.
- ⁴⁰ See Joy Buolamwini and Timnit Gebru, "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification," *Proceedings of Machine Learning Research* 81, no. 1 (2018): 1–15.
- ⁴¹ See, inter alia, O'Neil, Weapons of Math Destruction; Virginia Eubanks, Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor (New York: St. Martin's Press, 2018); Emmanuel Martinez and Lauren Kirchner, "The Secret Bias Hidden in Mortgage-Approval Algorithms," The Markup, August 25, 2021, https://themarkup.org/denied/2021/08/25/the-secret-bias-hidden-in-mortgage-approval-algorithms.

software that could sift through the reams of data accumulated and search for "patterns of life" that would help identify "terrorists" based on the behavioral data collected.⁴² Big Tech companies like Microsoft, Amazon, Google, Oracle, AT&T, Verizon, Cisco, Dell, Hewlett Packard, and IBM are also supplying the US military with technologies used for a wide variety of purposes, including surveillance.

By comparison to Global South countries like India and South Africa, in the West, biometric surveillance has been less widely accepted – perhaps due to the perception that biometrics surveillance is not for "civilized" people.⁴³ Yet biometric surveillance seems more commonly accepted today thanks to the rise of consumer use cases such as facial recognition and fingerprinting to unlock smartphones. As noted earlier, surveillance-driven consumer technology blurs the line between commercial and government surveillance. This is also true with new developments like "smart cities," which are often driven by sensors conducting big data surveillance of life in the city. In fact, many smart cities begin as "safe cities" projects in which smart camera networks, ShotSpotters, and other sensors are installed to monitor the streets. Once these technologies are in place, authorities aim to expand their use cases for city administration. Video cameras, for example, can be used to monitor waste disposal, cars on the road, and people flows to determine consumer foot traffic. Retail stores, airports, and other outlets are experimenting with video analytics to service, personalize, and manipulate consumer behavior.

While the development of new technologies and business models center in the Global North, the South is acutely subject to their dominance. As we see in Chapter 6, digital colonialism is the use of technology for the political, economic, and social domination of another territory. He United States has pioneered the technologies and business models now pervading the global digital economy, and US-based transnational corporations are dominant in most countries outside of the United States and mainland China. Simply put, digital technology is principally used to further the interests of American empire.

To achieve technological supremacy, US power elites and intellectuals must manufacture consent and pacify the public to accept American domination. This requires "tech hegemony" whereby the conceptualization of how technology could and should function in society assumes technology is owned and controlled by

⁴² Annie Jacobson, First Platoon: A Story of Modern War in the Age of Identity (New York: Dutton, 2021).

⁴³ Keith Breckenridge, Biometric State: The Global Politics of Identification and Surveillance in South Africa, 1850 to the Present (Cambridge University Press, 2014).

⁴⁴ Kwet, "Digital Colonialism: US Empire and the New Imperialism." For a take on data colonialism, a sub-component of digital colonialism, see, inter alia, Nick Couldry and Ulises A. Mejias, The Costs of Connection: How Data Is Colonizing Human Life and Appropriating It for Capitalism (Stanford University Press, 2019).

corporations and states.⁴⁵ As such, most people do not even try to imagine a fundamentally different, more egalitarian model for a tech society.⁴⁶ Western governments have so far pacified resistance to their mass surveillance programs by invoking the so-called "War on Terror" and national security interests while constraining policy to capitalist reforms. Transnational corporations branded themselves early on as fun and innovative, and as critics began questioning their power, the tech giants launched public relations campaigns professing their concern for human rights.

For example, Microsoft President Brad Smith co-authored a book on tech ethics and has made numerous public appearances attesting to Microsoft's alleged commitments to privacy and human rights. Microsoft has made press releases attesting to its "ongoing efforts toward racial equality," including donations to Black Lives Matter and other racial justice organizations, and, in 2020, pledged to stop supplying US police forces with (its own) facial recognition technology. However, Smith fails to mention in his publications and speeches that Microsoft has a Public Safety and Justice division that supplies surveillance technologies to carceral authorities and a Defense & Intelligence division that services intelligence agencies and militaries across the world.⁴⁷

Indeed, as noted above, Microsoft supplied its custom-built Microsoft Aware "Domain Awareness System" mass surveillance software to police in multiple cities. 48 Years later, Microsoft adapted its Aware surveillance platform for prisons, what it calls the Digital Prison Management Solution (DPMS), advertised at the UK government website. With the DPMS, prisons can ingest and process CCTV cameras, body-worn cameras, and tactical system data for applications like crowd control, perimeter breaches, and recorded incidents. Using surveillance devices, authorities can "virtually patrol a custodial community 24×7." The Solution provides "geospatial analysis," and claims it will "detect threats" by "aggregating massive amounts of data," "make data-driven decisions," "eliminate investigative silos," and "enhance intelligence capabilities" for things like "collabor[ation] with detectives, patrol, and other analysts." For prisons, Microsoft's DPMS appears unprecedented in scope and sophistication. Another Microsoft product, the Microsoft Advance Patrol Platform (MAPP), was developed for police patrol vehicles. The MAPP solution has been deployed as a pilot in Cape Town and Durban, South Africa. 49

⁴⁵ Ibid, 16-17.

⁴⁶ Michael Kwet, "The Digital Tech Deal: A Socialist Framework for the Twenty-First Century," Race & Class 63, no. 3 (2022); Michael Kwet, "People's Tech for People's Power: A Guide to Digital Self-Defense and Empowerment," RightzKnow (2020), www.rzk.org.za/wp-content/uploads/Peoples-Tech_August-2020.pdf; James Muldoon, Platform Socialism: How to Reclaim our Digital Future from Big Tech (London: Pluto Press, 2022).

⁴⁷ Brad Smith and Carol Ann Browne, *Tools and Weapons: The Promise and the Peril of the Digital Age* (New York: Penguin Press, 2019).

⁴⁸ In Brazil, police kill civilians at many times the rate of US police. See César Muñoz, "Brazil Suffers Its Own Scourge of Police Brutality," *Human Rights Watch*, June 3, 2020, www.hrw.org/news/2020/06/03/brazil-suffers-its-own-scourge-police-brutality.

⁴⁹ Kwet, "The Microsoft Police State"; Kwet, "Microsoft's Iron Cage." For an overview of how South African policing retains colonial and apartheid policies and structures, is often brutal and

Microsoft is also partnered to a wide range of surveillance vendors. A small sample includes Veritone, a supplier of facial recognition technology on the Microsoft Azure cloud available on the Microsoft website; DXC technology, which deploys prison software in major US counties; Kaseware, a surveillance platform similar to Microsoft Aware that offers mass surveillance capabilities and predictive policing; Netopia Solutions, a Morocco-based firm that offers Prison Management Software and sports features like "escape management." While it is not clear exactly where Netopia Prison Management Solution is deployed, Microsoft stated that "Netopia is [a Microsoft partner/vendor] in Morocco with a deep focus on transforming digitally, Government services in North and Central Africa." Morocco has a grotesque history of locking up journalists and dissenters, and torturing its prisoners. Netopia Solutions was a Microsoft "Africa Partner of the Year" in 2017, and its prison software is currently listed at the Microsoft AppSource website. 50

While Microsoft is far from the only company engaged in tech "ethics washing," it has been at the forefront of an effective PR campaign that has helped it escape the techlash. For decades, Microsoft has pumped money into the academic community, including major think tanks focused on tech policy and ethics, such as Data & Society and AI Now;⁵¹ academic institutions like New York University, Cornell University, the University of Washington, Strathmore University in Kenya, and the University of Witwatersrand in South Africa, among others; and it hosts its own set of Microsoft Research Labs spanning multiple countries. Esteemed Microsoft and Microsoftfunded researchers have taken up the topic of race and police surveillance, yet much like Brad Smith, they have erased, whitewashed, and downplayed the record of Microsoft's close relationship to authorities along the carceral pipeline, having failed to mention Microsoft's entire Public Safety and Justice division, vast array of partnerships, and wide variety of its own product offerings.⁵² Moreover, this same set of prominent researchers have failed to center the issues of digital colonialism and problematize the private ownership of the means of computation and knowledge, which reinforces the neocolonial domination of American empire.⁵³

Yet despite the influence of corporate money and public relations campaigns, scholars and activists are fighting back on more principled grounds. In the United States, the Athena coalition is protesting Amazon's police surveillance offerings and exploitative business practices. In Hong Kong, pro-democracy protesters tore down CCTV cameras and used laser lights to disrupt facial recognition. In South Africa,

racist, and generally supports the neoapartheid status quo, see Ziyanda Stuurman, Can We Be Safe? The Future of Policing in South Africa (Cape Town: NB Books, 2021).

^{5°} Kwet, "The Microsoft Police State"; Kwet, "Microsoft's Iron Cage."

⁵¹ Katz, Artificial Whiteness, 93–152. AI Now eventually dropped funding from Microsoft, but money from Melinda Gates's investment and incubation company, Pivotal Ventures, has also given money to Data & Society and became an AI Now funder after it stopped receiving funds from Microsoft.

⁵² Ibid

⁵³ Kwet, "Digital Colonialism: US Empire"; Cecilia Rikap, Capitalism, Power and Innovation: Intellectual Monopoly Capitalism Uncovered (New York: Routledge, 2021).

students and activists have attacked cameras and waged legal battles against smart camera networks, and are beginning to push back against digital colonialism.⁵⁴ In India, activists are also challenging digital colonialism and the expansion of police surveillance.⁵⁵ And in China, citizens have stood up to the private sector, demanding an end to invasive forms of commercial surveillance, including facial recognition.⁵⁶ These developments provide a glimmer of hope in a time of rapidly expanding high-tech repression.

This volume presents a timely intervention into the growing crisis of racial surveillance. While there are scores of valuable works on the advance of high-tech surveillance, much of it has been generated within the North and focuses on the US and Europe. This book, by contrast, takes a much-needed global approach to the matter. With contributions by twenty-four scholars from all over the world, the topic of race and surveillance is detailed across time and space. As we will see, racial surveillance spans the globe as a tool for oppression and exploitation.

In Chapter 2, Eric Stoddart sets the tone by exploring how surveillance technologies act as sociotechnological systems that construct and sort identity. Algorithms arrange people into binary categories that are resolved and discrete, rather than the fluid, messy, and multidimensional categories of real life. This creates conditions necessary to assess, predict, and control people according to their assigned identities, reinscribing unequal power relations between people of various identities in society.

In Chapter 3, Alfred McCoy lays out the historical and contemporary context of imperial electronic surveillance constructed by the United States. Starting with the conquest of the Philippines, McCoy shows the complex relationship between technological development for foreign conquest and the reuse of these technologies at home.

In Chapter 4, Toni Weller explains how surveillance was used to impose concepts of race on women in Victorian Britain. This is more than just a metaphor: British women were treated as Others of a different nature, as conceptualized according to prevailing notions of race, class, and gender/sexuality. Police were permitted to enter the houses of female persons under the guise of "hysteria" that was said to afflict women. Weller recovers oft-neglected history about the surveillance of women, who, like alleged racial groups, were said to differ in intelligence and character according to cranial measurements. A mix of pseudoscientific racism, class

Michael Kwet, People's Tech for People's Power: A Guide to Digital Self-Defense and Empowerment (RightzKnow, 2020), www.rzk.org.za/wp-content/uploads/Peoples-Tech_ August-2020.pdf. In 2022, the Friends of a Free Internet activist group launched a campaign for digital justice; see https://freeinternet.africa."

Megha Mandavia, "Activists Rally against 'Illegal' Surveillance of CAA Protests," Economic Times, December 31, 2019, https://economictimes.indiatimes.com/news/politics-and-nation/global-challenges-economy-up-on-rss-meet-agenda/articleshow/85930491.cms.

Jiayun Feng, "Viral Video of Man Evading Facial Recognition Leads to Surveillance Bans in Chinese Cities," SupChina, December 3, 2020, https://supchina.com/2020/12/03/viral-video-of-man-evading-facial-recognition-leads-to-surveillance-bans-in-chinese-cities.

discrimination, and bias against female sex work and sexuality combined with technologies of surveillance for the purpose of controlling women at a time when they were demanding more political and social power.

In Chapter 5, Amber Sinha and Shruti Trikanad take up the emergence of an electronic surveillance state in modern-day India. Sinha and Trikanad map out how British colonizers maintained "history sheets" about individuals accused, but not necessarily convicted, of a crime, and put on surveillance lists. Current attempts to digitize identity via the Aadhaar identity system, alongside e-governance programs and private sector commercial surveillance threaten to reproduce caste-based sorting of the Indian population according to race, class, religion, sex, place of birth, migration status, and disability in ways that undermine equality, civil rights, and civil liberties.

In Chapter 6, Michael Kwet traces how surveillance has been used from colonial conquest to the present in South Africa. Colonial and apartheid-era rulers utilized the latest and greatest technologies – from skin branding to fingerprinting to primitive computer systems – as a means to control and exploit the African population. The United States increased its involvement by supplying technologies in each era of white supremacist order, provoking opposition to firms like IBM, Kodak, and Hewlett Packard by anti-apartheid activists. In the post-apartheid era, US surveillance firms have reemerged through the process of digital colonialism for economic, political, and social domination.

In Chapter 7, Yasmeen Abu-Laban and Abigail B. Bakan explore Israeli surveil-lance against boycott, divestment, and sanctions activists. In the first part of the chapter, Abu-Laban and Bakan explain the BDS movement. Drawing inspiration from the anti-apartheid movement in South Africa, BDS activists have provoked the ire of the Israeli government, which finds itself under increasing pressure for its treatment of Palestinians by the international community. In the second part, the authors place responses by the Israeli state in relation to long-standing and still evident practices of surveillance and social sorting, as well as anti-Jewish, anti-Arab, and anti-Muslim racisms. They conclude with a reflection upon US and Canadian political landscapes and implications for antiracist movements and human rights policies.

In Chapter 8, Claudio Altenhain, Ricardo Urquizas Campello, Alcides Eduardo dos Reis Person, and Leandro Siqueira take on colonialism's legacy of race and surveillance in São Paulo, Brazil. The authors begin explaining the history of the *casa-grande* (the landowner's "big house") and *senzala* (the slaves' quarters), as well as the racialized order created during colonial conquest. They set forth the conditions to understand how today's prisons and *condomínios* (closed or gated communities) intersect with surveillance technology. Like elsewhere in the world, surveillance tech in São Paulo is reproducing the "quasi-colonial pattern" of racialized segregation in Brazil's largest and most global city.

In Chapter 9, Myunghee Lee and Emir Yazici unpack events in the Xinjiang Uyghur Autonomous Region of China. Lee and Yazici tell the history of Uyghur

civilization and how Han Chinese increasingly settled the cotton-producing area during the Mao era. In recent decades, the CCP has resorted to extreme forms of surveillance and repression to quell unrest in region. From facial recognition designed to detect Uyghur persons to forced "reeducation" and labor camps, the CCP has harnessed the powers of tech to maintain power and control.

In Chapter 10, we shift gears to the Global North. Frank Wu explains how Asian Americans have been treated as inassimilable into American society, whether by biology, culture, or collective choice. He tells the history of how Asian Americans have been discriminated against, Othered, and exploited for labor by systems of white supremacy. Wu brings the history up to date, using three case examples to show how Asian Americans now face renewed discrimination and surveillance due to ongoing tensions between the US government and China.

In Chapter 11, Anton Treuer brings us back to colonial America. Not surprisingly, surveillance was used by English settlers in the conquest of America. Treuer explains how tribes were surveilled, with maps drawn so the British could divide and conquer indigenous populations. By collecting census data and exploiting military intelligence, the settlers acquired the information needed for civilian and legal system expansion. By the early twentieth century, pseudoscientific cranial measurements and blood quantum standards were used to categorize indigenous people and deny them compensation for centuries of swindling. To this day, social services have maintained a close surveillance of native children, often resulting in them removed from their birth homes and placed into foster homes or adopted.

In Chapter 12, we take another look at indigenous North America, this time in Canada. Scott Thompson delineates how authorities used surveillance in colonial Canada to classify "Indian" peoples as a racialized Other and control their behavior. Recalling the history of British racial sorting in Canada, he explains how the English imposed a "natural" racial order that placed the English on top according to "God's plan." They classified indigenous persons to settle them in villages on reserves and assimilate them as inferiors in the racial hierarchy. Key programs and sites of surveillance included Indian Agents (indigenous government officials to oversee and manage the application of policy and law on reserves, using, in part, a paper permit system) and residential schools, as well as government surveillance of indigenous alcohol consumption.

In Chapter 13, Erica Nelson and Tracey Benson detail how policing in urban areas extends to Kindergarten–Grade 12 schools. Using Charlotte Mecklenburg Schools in the United States as a case example, Nelson and Benson show how the rise of mass shootings in American schools has led to a rise in federal support for school resource officers. The increased presence of police on school grounds increases the criminalization and incarceration of school-aged children for non-criminal behavior, with disparate impact on children of color.

In Chapter 14, Joel Busher, Tufyal Choudhury, and Paul Thomas explain how the UK government's strategy for preventing violent extremism, Prevent, has shaped 18 Michael Kwet

surveillance and monitoring practices in schools and colleges in England. Drawing on original empirical data from fieldwork, the authors demonstrate how these surveillance practices intersect with race, religion, and difference, with extra focus on Muslim students.

In Chapter 15, Anthony Cook traces resistance to racialized surveillance in American history, from abolition to Black Lives Matter. Beginning with slavery, Cook provides case examples, first focusing on slave fugitive Frederick Douglass as a prime example. He continues into the industrial age, where new technologies gave rise to new forms of surveillance – and resistance to it. The final sections of the chapter cover the Jim Crow era into the present.

In Chapter 16, Alana Saulnier provides a deep dive into the subject of how technologically mediated law enforcement in the United States may strain relations between police and racial minority communities. Saulnier argues that techno-fixes will not, in themselves, solve underlying issues of fractured community—police relations.