Introduction

Cryptopolitics and Digital Media

Katrien Pype, Victoria Bernal,
and Daivi Rodima-Taylor

Under President Joseph Kabila it became a criminal offense in the Democratic Republic of the Congo to have a SIM card that was not formally registered at the telephone company. In Kinshasa, rumor had it that this law was prompted by death threats the president had received via an *appel masqué* (phone call with a hidden ID). Anonymous threats were totally in line with the politics of intimidation that the Kabila regime enacted on its citizens via the secret service (ANR) and its network of spies who issued indirect warnings via text messages and were responsible for the disappearances of anti-Kabila protestors. Kinois (residents of Kinshasa) explained to Katrien Pype that someone most likely had bribed a telephone company employee to obtain the president's personal phone number.

While it is difficult to verify the accuracy of these statements, we take them seriously because crucially, these discourses involve contemporary imaginations of power as entanglements of unseen forces, including tech companies and state surveillance apparatuses that infuse communications with secrecy and suspicion. These power relations are steeped in mutual distrust between the parties involved such that communication is understood as a means of manipulation. The stories spun around the new law in Congo furthermore showed that citizens do not solely imagine themselves as subjects but also as agents in power games that rely on ambiguity, confusion, and deception.

We propose the term "cryptopolitics" as a way to draw attention to the significance of hidden information, double meanings, double-crossing, and the constant processes of encoding and decoding messages in negotiations of power relations. These manifest as secrets, hidden knowledge, allusions, insinuations, suspicion, obfuscation, ambiguity, skeptical

interpretations, and conspiracy theories, which are at the heart of social and political life.

Cryptopolitics is based on the premise of "depth," the assumption that there are various layers of meaning hidden beneath that which is said or shown (Barber 1987: 61–68). It involves the management of communication in ways that play off ambiguity and the distinction between concealed and overt information. It involves twin processes of encrypting and decrypting, the agentive practices of ambiguity, obfuscation, and dissimulation, and the engagement in practices of decoding, of trying to apprehend what is hidden, discerning the meaning, and the intentions and motivations behind the covering up.

The gap between the overt and the covert is a murky terrain; it is like a black box. Some may know what is actually hidden, while others do not. Secrecy and decoding are deployed to produce boundaries of exclusion and inclusion. Cryptopolitics, thus, are intimately entangled with inequality and difference. One of the basic underpinnings of any cryptopolitical agency is that some people are "in the know," while others are not, and should remain in the dark. Yet no one fully controls the meanings and interpretations others ascribe to the hidden and the obscured. That gray area is a subjunctive space: a space full of possibility and opportunity, but also of danger and risk as the chapters in this book show.

Cryptopolitics is not new, but it takes novel forms and has new consequences when it enters society through digital media. While digital media seemed to promise a new age of transparency and open access to information, it has also created new sources of ambiguity, opacity, and deception. The recent rise in fake news, conspiracy theories, and uncertainties about truth claims and science draw attention to powerful ambiguities manipulated for political ends. For example, the use of so-called dog whistles (secret symbols and words) by white supremacists in the United States and other extremists shows the complexity of the public and private because the public can be filled with hidden signs that constitute a form of private, secret communication (Am 2020; Drakulich et al. 2020, Weiman and Ben Am 2020). The internet and social media, moreover, increase possibilities for people to live fragmented, compartmentalized, or secret lives: they can appear as different people and inhabit different worlds online and offline. Digital media also introduce new layers of technological opacity; what goes on behind the screen as data is collected, transmitted, and stored, is invisible (Bernal 2020). The workings of algorithms and machine learning can produce results through processes that remain obscured even to those who designed them. As the 2022 crash of various cryptocurrency

platforms shows, even the ostensibly robust transparency of blockchains did not prevent swindling and theft, and perhaps even contributed to it as the claims made by cryptocurrency promoters created a false sense of security among buyers/investors.

Secrecy, deception, and ambiguity are not novel activities nor new objects of analytical inquiry (Simmel 1906, Taussig 1999, West and Sanders 2003), but cryptopolitics brings these kinds of activities into view under a unified conceptual framework that reveals how they are deployed politically. Cryptopolitics, thus, focuses attention on the workings of the hidden and the deceptive in relations of power. By "crypto" we draw attention to activities of concealment and revelation, and to the skills of encrypting, decrypting, coding, and decoding. By "politics" we highlight the power relationships and dynamics associated with secrecy, dissemblance, clandestine activities, and exposure. "Cryptopolitics" then encompasses the practices of producing confusing or ambiguous communication for specific purposes, and the hermeneutical strategies, practices of exegesis, and efforts to make sense of signs and forms that obscure, shield, and hide.

New forms of cryptopolitics emerge with digital media, including the veiled, complicit partnerships between states and technology companies, enabling surveillance or internet shutdowns in times of elections or other tense political moments, as happens frequently in Africa and throughout the Global South. A growing number of states rely on telecommunication and technology companies to help limit the circulation of information that threatens their political power. States also seek to use data collected by tech companies for various political ends. In both these efforts the official rationale is often that of "security," a paramount contemporary domain of cryptopolitics since threats and espionage produce and are produced by secrecy and suspicion.

Encryption and decryption have gained prominence as technological issues, but through cryptopolitics we analyze them as cultural phenomena. In the contemporary world, the skills of concealment, ambiguity, and subterfuge as well as the skills of discernment and interpretation are both social and technological. Political conflicts, elections, repression, and revolt, along with other political flashpoints bring cryptopolitics dramatically to the fore. Everyday interactions and interpersonal relationships are also fields for cryptopolitics as people increasingly manage their relationships with others through revelation and concealment, especially as they conduct their lives across online and offline worlds. What needs to be hidden from whom, and what gains power or protection from being hidden, and who is able to decipher ambiguous communications depends on the social and political context. Ethnographic

research and anthropological perspectives thus are key to understanding the dynamics of cryptopolitics in any given context.

Cryptopolitics is a lens that helps bring into focus a dynamic of power and communication that operates in a wide array of settings. This anthology explores cryptopolitics in diverse African contexts through ethnographic perspectives and in-depth qualitative studies. The authors situate their work at the intersection of cultural anthropology, media studies, and African studies.

Cryptopolitical Perspectives in Anthropology and African Studies

Cryptopolitics means strategically saying one thing, but meaning another, or showing one thing, while concealing something else. Strategic, enigmatic locutions are "thick" (multilayered), where meanings lie beneath the surface for those who have the skills to interpret and read between the lines, while the naïve may take them at face value. Cryptopolitics foregrounds these processes whereby information is hidden or made ambiguous, and communications contain indirect, symbolic, and secret meanings to be interpreted. These processes are entangled with power and powerlessness, with political intent or consequences.

While the issues of secrecy, deception, allusion, and hidden meanings are central to much of anthropology, the concept cryptopolitics is not. To date the term has only appeared in anthropology in a 2012 publication of *Arizona Anthropologist* authored by Raymond Orr who was a graduate student at the time (Orr 2012). He writes about the Isleta Native American community where he conducted fieldwork: "Isleta politics are well-hidden. Individual and group bellicosity takes the form of crypto-politics. These types of politics express themselves non-politically through forms of social subterfuge. Disagreements, hurt feelings, desire and senses of injustice are part of Isleta communal life but the particular community norms allow bellicosity to be expressed openly only at high cost to participants" (Orr 2012: 61). Orr adds that "conflict and where it is (and is not) acknowledged is complicated for both those in the communities themselves as well as the scholars who study them" (Orr 2012: 61).[1]

Orr mentions the influence of political science on his approach but does not cite any source for "crypto-politics." The earliest usage and perhaps the coinage of the term dates from a 1965 article by political scientist T. H. Rigby. Rigby (1965) used "crypto-politics" to describe the political system in the Soviet Union where public politics were state-orchestrated or suppressed, and where processes of official decision-making were

hidden behind a façade of institutions. As anthropologists, both Orr and the contributors to this volume extend cryptopolitics beyond the state to encompass a broad range of power relations.

Orr goes on to suggest that Isleta's initial "tranquility," which he depicted at the essay's outset, is possibly enforced by secret forms of conflict such as slander, rumor, and even accusations of witchcraft. Orr thus captures the very essence of cryptopolitics that we have conceived here. It is about deceptive appearances, secret and ambiguous communications and "politics" that takes indirect and unconventional forms. As James Scott (1985) has pointed out, besides overt acts of resistance such as organized rebellions, the less powerful often turn to subtler acts of non-cooperation. These everyday forms of resistance may include evasion, strategic ignorance, or non-compliance, and frequently contest the "public transcripts" of formal hierarchies through a "veiled discourse of dignity and self-assertion" (1985: 137; see also Scott 1990). While such "weapons of the weak" are often cryptopolitical in character, cryptopolitics are employed by the powerful as well.

A few works outside the discipline of anthropology have used the concept of cryptopolitics. Ananya Kabir (2014) rather uniquely connects cryptopolitics to the crypt in her analysis of Kashmiri resistance and cultural production around the body, the grave, and martyrdom. But scholars have usually understood this concept in a much more literal manner to mean the politics surrounding digital encryption and/or the internal power dynamics in the blockchain developer community (e.g., Groos 2020; Monsees 2019). There is a history of conflict over the uses and spread of encryption, sometimes referred to as "cryptowars" (Hellegrean 2017; Jarvis 2020). Such struggles show, as we explore throughout this volume, that concealing and revealing both involve power. The controversies surrounding Julian Assange, WikiLeaks, Chelsea Manning, and the revelations by Edward Snowden are indications of the global significance of hidden knowledge, clandestine communication, and the powers of revelation associated with the digital (Hintz, Dencik, and Wahl-Jorgensen 2017). In that sense, we may inhabit a particular cryptopolitical condition—one that is facilitated and amplified through digital media.

Our chapters all share a focus on Africa. There are compelling reasons why ethnographies of African digital cultures provide fertile ground for the exploration of cryptopolitics. The first is that in certain African contexts indirectness and the cryptic have been preferred forms of communication. For example, in her seminal article on popular arts in Africa, Karin Barber (1987: 8) writes that "works which appear conservative . . . may conceal criticism of, or reservations about, the status

quo which people have good reasons not to express openly. They often reveal doubts and anxieties; and possibilities of an alternative view appear in textual loopholes, fissures, and silences." Second, conspiracy theories thrive in postcolonial Africa, where citizens have a long history of distrusting their leaders, and where they struggle to make sense of political pronouncements and events that they find confusing or suspect. Third, Africanist anthropology has an enormous archive on the occult and the invisible realms in cosmological worldviews, in which believers can only try to understand the world by interpreting signs. Fourth, digital media, consumed mostly through smart phones, has rapidly become central to African politics and social life. As is the case in the rest of the world, African states, private companies, humanitarian organizations, religious communities, families, and other networks rely on digital technology in one way or another.

Furthermore, sorcery and magic, two key rubrics in africanist anthropology, are cryptopolitical behavior because these actions depend on a deliberate manipulation of material reality by invoking hidden, occult powers. The complexities of studying the political dimensions of the hidden and the occult in the current era of neoliberal globalization can be illustrated by the example of the "occult economies" of post-apartheid South Africa (Comaroff and Comaroff 1999). As the impoverished masses witness vast wealth passing to the elites through the hidden speculations of the neoliberal market, some people resort to novel magical means in pursuit of their goals. Their practices, often parodying the free market, find expression through a variety of contemporary media—including "dial-in diviners" and multimedia ritual technologies. The proliferation of "mystical arts" in postcolonial Africa should not be viewed as a retreat to the traditional past, however, but rather as employing culturally familiar tropes and technologies to produce new ways of coping with contemporary inequalities: a "new magic for new situations" (1999: 284). Such populations that are disenfranchised or marginalized politically as well as economically seek sources of power in the occult while also suspecting that elites use such powers to achieve the positions they hold. Witchcraft accusations are closely related to practices of decoding, where signs must be deciphered to uncover hidden, spiritual machinations. Yet clearly cryptopolitics is not solely an African phenomenon. Practices of encoding and decoding are part and parcel of social life anywhere around the world.

Cryptopolitics is not a new phenomenon that has only emerged with digital media. Rather, discussions about encryption, fake accounts, deep fakes, and disinformation remind us that deliberate confusion, double-speak, allusion, suspicion, distrust, and deciphering are often part of

human interaction, and are always embedded in strategies of power. At the same time, we should keep in mind that cryptopolitics is foundational to the digitized world, as technologies amplify the duality of concealment and revelation, and also magnify the scale, scope, and set of stakeholders associated with any particular instance. With this book, we introduce the concept of "cryptopolitics" as an analytical space that is fruitful for new investigations in contemporary power configurations. We hope that the chapters of this volume can serve as an inspiration to engage in similar research beyond the African continent.

Secrecy and Cryptopolitics

Our lives are made up of relationships, moments, utterances, and experiences in which ambiguity, doubleness, and indeterminacy may be cultivated, appreciated, and explicitly sought after. In other instances, these same characteristics are considered threatening and deceptive, prompting suspicion and efforts to decipher hidden truths. Navigating powerful institutions and everyday social life means constantly calibrating the desirability of transparency or opacity, of disclosing more or less information, and, on the other hand, continually assessing the real import of information one is given. Scholarly attention to cryptopolitics thus brings nuance to the study of secrecy, which very often seems to be understood as the radical opposition of full transparency or full opacity. We consider these two modalities to be opposite ends of a continuum, with most of life taking place between them, where concealment and revelation work together in a range of informational practices depending on the context.

Secrecy, ambiguity, and dissemblance mediate nexuses of power and knowledge. There is power in keeping things hidden and power in gaining access to what is hidden, as well as in being able to interpret what lies beneath the surface. Regulating exposure is essential for constructing "intersubjective and institutional life" (Manderson et al. 2015: 183), yet hiding and concealing are practices that leave traces. The existence of secrets or hidden agendas is often known, suspected, and made manifest either willfully or inadvertently. It is important therefore to view encoding and decoding practices through their performative aspects, with attention to the ways valued information and knowledge are concealed, imparted, or deduced through increasingly diverse communicative practices and interpretive skills. This underscores the processual dimension of such concealed content—the establishment of secrets and the occasion of their revelation invest them with social force (Jones

2014; see also Herzfeld 2009). Instances and practices of disclosure and of interpretation should therefore be seen as political, in fact, as cryptopolitical.

Secrecy is also sometimes described as silence—as if keeping secrets just means not talking about something. With our notion of "cryptopolitics," we want to unsettle that taken-for-granted correlation between secrecy and silence. An analytical focus on cryptopolitics shows that much is actually said while hiding something else. People use veiled language, speak in indirect fashion, and downplay one thing by emphasizing another. In many of our interactions, we are constantly producing partial truths. The notion of "partial truths" has gained particular salience in anthropology to refer the fact that claims and narratives always come from a particular positionality (Clifford and Marcus 1986). But it is also the case that certain utterances are purposely chosen in order to avoid other, riskier statements, and thus keep that information, those experiences, emotions, and opinions hidden. Here we draw attention to the fact that certain statements, testimonies and confessions, and other narratives may disclose specific parts of significant data, while the speaker may choose to obscure other parts. The calibration of transparency and opacity that makes up a significant part of any cryptopolitical action occurs in intimate lifeworlds, in political communication, in economic transactions, in religious practices, and in artistic expressions. It involves the speaker's agency, their assessment of the communicative context, and their repertoire of communicative resources and skills, and triggers the agency of the audience in determining what is being obscured and why.

Cryptopolitics can take many forms (see below). Apart from the deployment of irony, figurative speech, and other discursive forms, gestures can also be mobilized in cryptopolitical activity. Within anthropology, the wink is probably the best-known symbolic gesture. Generations of students have been trained in our discipline's signature method of participant observation by learning about Clifford Geertz's distinction between the blink of an eye and the wink (1973). The latter is a socially significant act that differentiates within a group of people by bodily communicating common knowledge and a shared perception. The shared understanding of a wink among those in the know could be considered cryptopolitics on a micro level.

Whispering, in its literal and its metaphorical sense, is another cryptopolitical gesture. Just like ironic utterances and the wink, the whisper materializes the double layering of how information is often managed. The whisper produces sound that is only intelligible to a limited group of people, and thus makes audible the boundaries between those who

should know and those who should not know. The act of hiding is made manifest in a very sensuous way.

The whisper has become a powerful sign in the Global North where various idioms emerged around it, for example a neologism such as "whisper networks" (Babel 2018). Commonly, whisper networks reference chains of informal information-sharing among women, who exchange knowledge about marginalization, violence, and vulnerability, in an attempt to provide protection against male abusers. Whisper networks highlight a form of resistance through hidden disclosure; they arise from an uneven distribution of the power to speak along gendered lines. They are thus manifestations of cryptopolitics in a society where powerful men dominate not only many industries but also formal systems of justice.

Distrust, Duplicity, and Discretion

Cyptopolitics is always a social practice, embedded in relationships, and therefore it is the privileged terrain of anthropological inquiry. Overall, cryptopolitics is deeply entangled with trust and distrust. Hiding and obscuring information, intentions, and affects may be inspired by a lack of trust toward the receivers, whether they are intimate others, political agents, or non-identified actors of global power configurations.

Relations of distrust are often characterized by duplicity. Double speak, fake accounts, and disinformation may at once be symptoms of distrust toward certain authorities or audiences. At the same time digital media itself generates distrust. There is growing global desire to share information in end-to-end encrypted environments evidenced by the massive growth in Signal and Telegram accounts in early 2021 after WhatsApp announced that it would share data with Facebook (WhatsApp started in California in 2009 and was acquired by Facebook, now Meta Platforms, in 2014). This backlash against WhatsApp seemed to be inspired by distrust in Facebook, which had been sharing users' data with other private companies and sometimes with repressive states.

Yet, distrust often governs interpersonal relationships and relations to and among institutions as well. Experiences of doubt about other's intentions and motives generate suspicion and conspiracy theories. This plays out strongly in Africanist research, where uncertainty, confusion, and distrust have become tropes in the study of social and political life (Cooper and Pratten 2015). Unstable economies, authoritarian regimes with whimsical political leaders, and lingering civil wars have instilled a distrust between people and their leaders, and also among citizens themselves (Bernal, this volume). Practices of hiding and shielding have

been explored in urban Africa, where pretense and bluff, for example in Inhambane, Mozambique, and Abidjan, Ivory Coast, are applauded as necessary strategies for social advancement (see Archambault 2017; Newell 2012).[2] Furthermore, social codes that hide uncomfortable truths reign.[3] Such contexts instill a basic sense of doubt and skepticism toward what is said and shown, as people expect that others are actually hiding difficult truths.

Efforts to hide uncomfortable truths have also been observed where certain medical conditions are stigmatized. People may engage in a wide range of cryptopolitical strategies to conceal health problems. Relatives and friends may cooperate in these efforts to dissimulate as research on HIV care in Burkina Faso and Zambia has shown (Hejoaka 2009; MackWorth-Young, Bond, and Wringe 2020; Rhine 2014). Vague language, figurative speech, and other indirect locutions may signal the desire to be discrete. Crucially, in such contexts, people may understand and therefore refrain from asking questions.

In contexts where taboos, stigma, and repression are most heavily felt, cryptopolitics plays a larger communicative role. In such instances, duplicity is not linked to treachery, but to discretion. Whispers, winks, and coded language manifest complicity, a relationship thriving on shared knowledge, while outsiders do not have access to that information. Duplicity may be a way of avoiding the power of others or a way of exercising power over others.

Exposure and Disclosure

Of course, where there is discretion, there are also restricted groups or communities of people where the secrets can be aired. For example, in Bedouin worlds (Abu-Lughod 1993), women's songs reveal their "veiled sentiments" through indirect expression not every listener comprehends. They engage in doublespeak to protect dominant power hierarchies, while nevertheless expressing their opinions and feelings. Ethnographies of mental health draw attention to practices of information management that border on cryptopolitics. Central to the care of the self are processes of sharing private emotions, traumas, and anxieties with others suffering from the same affliction or with therapists. Therapeutic support groups work in part by allowing hidden knowledge to be expressed in a ritualistic context (Kitanaka 2015).

Privacy, or the identification of the boundaries between the private and the public, is one of the social domains where cryptopolitics comes

to the fore. Ultimately, social life resides in a paradox: insofar as secrecy produces social boundaries, the very existence of the secret is public knowledge. Boundaries between "those who know" and "those who do not know" (or "those who ought to know" and "those who should not know") thrive in any society. These boundaries are policed: practices are put in place in order to protect them, while protest, contestations, rumors, and leaks challenge these boundaries. Anthropological work often involves trying to understand how such boundaries are materialized, preserved, and transgressed or transformed. Cryptopolitics offers a purchase on these relationships and processes with particular attention to their power dimensions and to the significance of ambiguity and double meanings.

Several African societies have idiomatic expressions addressing the necessity of only partial transparency. In Kinshasa, the proverb *toyebi motema ya batu te* (we can never know what is in the hearts of others, Pype, this volume) warns that relatives, friends, neighbors, or strangers may not always have the best intentions, and full disclosure is risky. In Burundi, the term *ubgenge* denotes cleverness in indirection or dissimulation, a strategy of "hiding just enough" and "revealing just enough" of one one's own intentions and/or the intentions of others (Turner, this volume). Such ethnographic examples show how cryptopolitics works through a balance between opaqueness and disclosure.

The #metoo movement that spread across the globe in recent years is another testimony to the power relations that often compel secret-keeping and pretense on the part of the vulnerable (Chandra and Erlingsdóttir 2020). It can be seen as a cryptopolitical phenomenon in that it not only revealed how widespread the practice of secrecy surrounding sexual abuse was but also called for the unveiling of negative truths about powerholders. All these observations show that in private and public life full transparency or exposure means vulnerability.

The affordances of digital media and social platforms are significant here because of the ways they allow users to scale between full exposure and discrete communication. Parameters within platforms such as WhatsApp, Facebook, and other apps require users to think about their publics and social networks and to deliberate about the scale at which they want particular content to circulate online (though these controls themselves obscure the ways Facebook uses people's data). Digital media also make it easy for people to secretly make audio/video recordings of conversations or activities and to share these fully or in snippets (whether edited or not) online. In order to avoid context collapse (or the possibility that non-addressees also read a particular post), users

sometimes post "images with references comprehensible to some of the viewers but not others" (Miller et al. 2016: 175). People may also manage their images and reputations or seek to manipulate audiences through the use of pseudonyms, fake accounts, and doctored images. VPNs (virtual private networks) are sometimes used to hide a person's location, while the Tor network can conceal a person's browsing activity. Digital media, moreover, (from social media content to the Google search function) offers people access to a highly curated, subjective slice of data and information—which is frequently presented as objective and understood to represent the full picture.

Though, as Cambridge Analytica so dramatically revealed, the control people think they exercise over digital information is often illusory (Hinds, Williams, and Joinson 2020). The encryption practices advanced through social media platforms, when linked for instance to fintech and banking, may create exploitative invisibilities such as data capture and "Ponzi" schemes, as shown by Daivi Rodima-Taylor (this volume). The compilation and use of big data is creating new opaque zones of power and establishing potent invisibilities embedded in growing disparities of expertise and access, which may lead to new social inequalities (Nuttall and Mbembe 2015).

As cultural anthropologists, we are mainly interested in people, communities, and institutions that are engaged in processes of encoding and decoding. Yet, several of our contributors draw attention to the nonhuman actors in cryptopolitics. Lisa Poggiali (this volume) describes how new biometric technologies of population regulation encode and decode information about bodies, citizenship, and belonging. These biometric data do not always result in transparency, however, but lead to new forms of concealment or evasion. The risk of ethnic and racial discrimination arising from limited inputs that create bias in software programs is well known. The fixing of identity through biometrics can also have dire political consequences for affected groups. While technologies can sometimes work to solidify and fix identities to negative effect, other times they can be used to construct more fluid and multifaceted identities. Such technologically mediated identity creation is cryptopolitical; seeking, on the one hand, to exercise political power through revealing what is viewed as an essential identity, and on the other hand, engaging in political resistance by manipulating and subverting assigned identities. Peter Chonka (this volume) draws attention to the algorithms used by search engines that through their auto-completion features suggest clan identities as search terms for any search involving a Somali name. In doing so, search engines may influence perceptions and constructions of Somali identity.

Infrastructures of Cryptopolitics

Diverse material and immaterial infrastructures undergird cryptopolitics. Digital media has enabled transparency, but it has also enabled opacity, anonymity, the dark web, and new forms of deception and manipulation (Bernal 2020; Beshiri and Susuri 2019; Coleman 2014). Institutions are both material and cultural, including big technology companies, startups, universities, research institutes, local governments, and states. All these are mobilized by social and political actors engaged in hiding or exposing data and information, while technical affordances, skills, and access vary—thereby contributing to exclusions and inequality. The specific constraints and affordances of applications, platforms, algorithms, mobile phones, and modes of digital media such as videogames, and various other devices and infrastructures can be seen as providing material bases for cryptopolitical activities. Our anthology therefore contributes to the broader study of communicative infrastructures as socio-technical assemblages with their material, ideational, and peopled dimensions (see also Bernal 2021; Rodima-Taylor and Grimes 2019, Rodima-Taylor 2021).

While European governments enforce some data protection measures on digital communication providers, various African countries often create regulatory carveouts that undermine the use of encryption. Security—whether national or public—is often the stated reason for legislation that limits anonymity and the use of encryption so as to combat terrorism and crime, but such measures also squelch protest and political opposition and limit freedom of speech and assembly. In various African countries and beyond, the use of encryption is restricted in order for states to monitor political opponents, journalists, and human rights defenders. Registration and licensing of encryption service providers are mandatory in many African countries, and failure to hand over secret encryption codes to state authorities, or using prohibited encryption tools can lead to enormous fines and imprisonment. Regulators and other government agencies thus easily gain access to decryption keys and encrypted data (CIPESA 2021).[4] Digital technologies have also fostered new surveillance and security measures used by states and private companies. The stockpiles of data are powerful public secrets that are known yet hidden from citizens, a form of cryptopolitics. The objection of African governments and the US government to the encryption of communications is testimony to the power that rests in information and in data. Struggles over who controls what is known, what can be revealed, by whom and to whom are being waged globally.

Such new power formations lead to new power struggles, as the tensions between the European Union and American platform companies show. They also generate new strategies and tactics of resistance. All over the world, to varying degrees, people engage in new, digital, and non-digital practices in efforts to escape repression and retain some privacy—whether they are responding to the state, other authorities, or surveillance capitalism (see also Couldry and Mejias 2019; Zuboff 2019).

Cryptopolitical Aesthetics

The digital world offers new terrains for engaging in strategic play with the gap between the said and the unsaid, the surface and the depths. The ongoing proliferation of new media affords new strategies of secrecy and doublespeak, and new grounds for suspicion, while demanding greater skills of encoding and decoding. These have multimedia dimensions as they are manifested across a variety of domains and materialities—highlighting the need to explore them across a variety of media and in the contexts of both social and material realms of particular cultures and societies (Jones 2014; see also Ferme 2001; Rajewsky 2005). Digital encryption itself, or the translation of plaintext into ciphertext (unreadable by a human or by a machine without the cipher), may be understood as privacy or may be understood as clandestinity, a means of keeping secrets that could be dangerous.

One of the most inspiring discussions of "digital depth" is Jennifer Deger's analysis of Yolngu digital practices (Deger 2016). Yolngu mobile phone users produce "spectral depth" by creating digital images with Greenscreen software, montage and GIF effects. These generate layered images and allow Yolgnu people to "creatively participate in a profoundly synaesthetic and sentient world, a world enlivened by uncanny encounter" (2016: 111). Key here are the "inside meanings" in a world "that far exceeds the registers of what the eye can see, the camera can capture, or indeed, what the anthropologist will ever know" (2016: 116). The ostensible factualness and truthfulness of a photographic image that is often assumed turns out to be an illusion.[5]

Digital tools such as cropping, zooming in, adding markup text and arrows, and bringing photos together in a collage allow digital users to draw attention to the hidden and to read different layers of meaning into a political event, text, or performance.

Humor and public secrets may provide one of the most surprising infrastructures of cryptopolitics. Both genres of social communication

draw on a collective understanding that there is a gap between the said and the unsaid; there is something that for one reason or another cannot be expressed explicitly. Postcolonial African regimes thrive on doubleness (see Bernal, this volume; Mbembe 1997), and cultural formats that cultivate doubleness may therefore flourish in such political cultures. It may not be a surprise, therefore, that humor and rumor (see Bernal, this volume) have been major themes in African studies (Barber 1987; Obadare 2016; B. White 2007; L. White 2000). Insofar as many postcolonial African regimes have tried to suppress antagonistic voices while broadcasting their own propaganda, citizens deploy humor and rumor, cultural genres that thrive on anonymity, insinuation, and double meanings, as means of alternative storytelling. It is through humor and rumor that other "real" versions of events can be exposed.

Conspiracy theories are another genre associated with cryptopolitics. The premise of any conspiracy theory is that certain realities are hidden and need to be made manifest to larger publics. The digital sphere becomes an additional space in which citizens can expose the various forms of hiding and obscuring of their state or where subalterns can contest their leaders anonymously. It is probably no coincidence that humor, rumor, and conspiracy theories make up large parts of digital content. Several of our ethnographies indicate that African citizens are profoundly aware of how their states perform a politics of deception. Citizens respond by communicating in hermeneutical genres such as rumors and conspiracy theories.

Cryptopolitics may also work through religious culture and genres. Many religions cultivate a variety of genres of decryption and disclosure that engage with notions of doubleness. Religious leaders and practitioners often understand their worlds as bifurcated between a visible and an invisible world. Mediation between the two spheres is often the privileged province of religious leaders, who thus obtain much power and influence over their community. In addition, many religious communities have installed experts, rituals, and cultural genres to safeguard the boundaries between the visible and the invisible, the material and the transcendental. Pentecostal-charismatic Christianity, which has gained much prominence in Africa since the 1990s, thematizes exposure and revelation. Witchcraft films in Ghana (Meyer 2015) and evangelizing TV-serials in Kinshasa (Pype 2012) are genres that foreground processes of decoding. Filmmakers construct plots that revolve around the identification of evildoers, after they have caused mishap and distress in the lives of the protagonists. Sermons, another genre of Pentecostal-charismatic Christianity, often contain decryption of biblical verses or tales, and pastors engage a discourse in which they claim to reveal

messages that are hidden in the Bible (Pype 2011). Sermons and confessions are embedded in power hierarchies. Confessions involve strategic revelations as the confessees, marginal figures in the community, admit their transgressions while announcing they have changed in order to be accepted in the Pentecostal community. All of these examples suggest the range and diversity of contexts in which cryptopolitics play a part.

Overview of the Chapters

This anthology brings together original research on diverse countries in Africa and diasporas, including Somalia, Eritrea, Burundi, Kenya, Tanzania, Mali, South Africa, and the Democratic Republic of Congo. All of the chapters examine the role of emerging digital technologies and platforms in mediating knowledge production, with a focus on cryptopolitics—the coding of messages and unveiling of hidden meanings in negotiations of power, identity, and legitimacy. A common theme is the relationship between the state and society with particular attention to conflicts, migration, ethnic rivalries, and authoritarian systems. The diasporic and transnational dimensions of belonging and governance are another focal point of the anthology. The analyses are based on original empirical material and demonstrate the multidimensional aspects of cryptopolitics that transcend and interweave online and offline, public and intimate socialities, and formal and informal spaces. The chapters demonstrate how political and social practices are always anchored in local sociality, and show that the analysis of the role of social media in contemporary Africa is frequently crucial for understanding the cryptopolitical dynamics between the powerless and powerful.

Katrien Pype presents an analysis of the cryptopolitics embedded in the tension between the visible and the hidden in Congolese digital media. The local concept *benda bilili* or "pulling images" conveys a specific "aesthetic of ambiguity" that characterizes the digital universe of Kinshasa. Cryptic communication among Kinois involves socially conditioned strategies of limiting the amount of information conveyed and interpreting the limited information provided by others. Concealment constitutes an important strategy for managing personal relationships. The enigmatic online posts that are rapidly becoming a norm in Kinois digital and social media space also provide new tools to deal with the "vulnerability of human sociality" in offline realms.

Simon Turner reveals the increasing role of social media in the culture of cryptopolitics in Burundi, where selective concealing and

revealing of information has long been part of social and political strategies. Digital media have afforded new forms of interaction between the state and its citizens in a context where ethnic conflict and contestation simmer under the surface of the country's politics. The practice of concealing emotions and information, peculiar to Burundian royal courtiers of the past, fosters an online culture where people search for what is hidden, and engage in strategies to sound out adversaries. Social media afford public visibility to debates and critical opinions, enabling protagonists to elicit responses from the public and force people to take a stand on contentious issues. Digital media thus serves as an important cryptopolitical tool of unveiling the hidden in this context.

George Ogola examines cryptopolitics in the exchanges among Kenya's online publics, arguing that digital platforms like Twitter have disrupted the economies of control that have traditionally governed the circulation of information in the country. Ogola traces the hashtags of "Kenyans on Twitter" as they draw from the "disorder" of everyday life and shape new debates and practices of engaging with institutional politics. Calling for a broader view of politics as "dispersed and infra-institutional," Ogola reveals how Twitter conversations assemble novel "pockets of indiscipline" that incorporate more inclusive discursive practices. Yet digital platforms also create opportunities for the establishment of a new repressive information regime by the Kenyan state.

Marie Deridder and Olivier Servais address cryptopolitics in their analysis of the video game *Muslim Mali*, which was set and being played in the context of an ongoing conflict in Mali. The game positions the player as a Muslim Malian shooting down French fighter planes. The game played into the growing social unrest and rejection of elites and a surge in Islamic groups and militants. The chapter explores how Western media reactions to the Muslim Mali game drew on narratives of African otherness. In contrast, Deridder and Servais present a detailed analysis of the complexity of political events and actors in the Malian conflict. Instead of a simplistic opposition between African Muslims and the West, the analysis reveals the complexity of regional and global power assemblages with their geopolitical interests.

Peter Chonka focuses on the political interactions of the conflict-ridden Somali state and its global diaspora with the virtual digital publics mediated by an array of local and global media networks. Chonka's detailed analysis of the actors mediating Somali conflict in physical space considers national and regional militias, international recruits from the African Union's Mission to Somalia, as well as diverse "media producers" such as local public and private broadcasters that are intertwined

through global social media platforms such as Facebook and Google. Tech platforms not only play a role in cryptopolitics through the circulation of conspiracy theories, but also through their auto-completion features that often suggest clan-related keywords for searches involving Somali names.

Daivi Rodima-Taylor explores the cryptopolitics of digital chat apps that have become widespread in Africa. The apps accommodate large groups as well as enable private, encrypted chat messaging on their platforms. Such apps are increasingly central in mobilizing online savings groups and migrant remittances; they are also used for fundraising for a variety of causes. Drawing on empirical material from South Africa and Kenya, the chapter explores the paradoxical partnership between WhatsApp as a BigTech platform and these informal economic initiatives. Rodima-Taylor discusses the novel questions this poses about digital media and civic spaces in Africa. She analyzes the cryptopolitics of these emerging pathways of digital mutuality that, while building on vernacular organizational templates and facilitating alternatives to formal banking, also create exploitative invisibilities and foster data capture, while giving rise to scams and Ponzi schemes.

Victoria Bernal analyzes the ways people in Eritrea and among the diaspora regard the dictatorship of Isaias Afewerki through a prism of humor. She argues that the double meanings and ambiguities of humor resonate with the cryptopolitics of dictatorship. Reflecting on questions of political repression and the limits of internet freedom, Bernal suggests that such humor and mistrust are products of extreme repression. The pervasive sense of surveillance produces a constant awareness of the need to conceal and of the presence of duplicity. The political humor in people's everyday conversations and in online media that is out of the reach of the state constitute diverse forms of politics. Humor unveils the ambiguities and inconsistencies in official narratives and figureheads and exposes these to public scrutiny and questioning.

Lisa Poggiali examines the emerging strategies of digital governance that seek to render refugee identities legible to security systems in Kenya. The Kenyan state presents biometric identification measures as necessitated by threats posed by Al Shabaab, for example. The state faced international pushback when it tried to implement overt policies restricting refugees, so it has turned to indirect strategies of control through procedural measures, including the registration of refugees' sim cards and biometric technologies of identification. Poggiali also explores the digital strategies used by refugees to evade or redirect the gaze of the Kenyan state. New technologies of population regulation

enable new ways of encoding and decoding information about bodies and citizenship, often limiting refugees' movement and legal status, but also providing novel ways for refugees to create alternative configurations of security and sociality.

Victoria Bernal is a cultural anthropologist whose scholarship in political anthropology contributes to media and IT studies, gender studies, and African studies. Her work addresses questions relating to politics, gender, migration and diaspora, war, globalization, transnationalism, civil society and activism, development, digital media, and Islam. She is Professor of Anthropology at the University of California, Irvine. Bernal's articles and chapters have appeared in various collections as well as in anthropological, African Studies, and interdisciplinary journals, including *American Ethnologist, Cultural Anthropology, American Anthropologist, Global Networks, Comparative Studies in Society and History, African Studies Review,* and *Political and Legal Anthropology Review.*

Katrien Pype (associate professor at KU Leuven, Belgium) is a cultural anthropologist, mainly exploring media, popular culture, and technology. She has written about the production of television serials, television news programs, TV dance shows, and long-distance communication, all in the context of contemporary Kinshasa. Her work is published in edited books, and in journals such as *Africa, Ethnos, Journal of the Royal Anthropological Institute, Journal of Modern African Studies, Journal of African Media Studies*, and others. Her monograph, *The Making of the Pentecostal Melodrama: Religion, Media, and Gender in Kinshasa*, was published with Berghahn Books (2012). Pype also co-edited, with Jaco Hoffman, *Aging in Sub-Saharan Africa: Spaces and Practices of Care* (Policy Press, 2016).

Daivi Rodima-Taylor is a social anthropologist and researcher at the African Studies Center of the Pardee School of Global Studies of Boston University. Her research focuses on African informal economies, financial technology and social media platforms, and migration and remittances. She has conducted longitudinal field research in East Africa and published in journals including *Africa, African Studies Review, Global Networks, Social Analysis, American Ethnologist, Journal of International Relations and Development, Environment and Planning: Politics and Space, Geoforum, Global Policy,* and *Review of International Political Economy.* Her recent publications include the co-edited volume *Land and the Mortgage: History, Culture, Belonging* (Berghahn Books, 2022) and the co-edited special issue *Fintech in Africa* (*Journal of Cultural Economy*, 2022).

Notes

1. Orr considers cryptopolitics reflexively in relation to Native American Studies where he found a "taboo" on researching intratribal conflict as opposed to conflict between Native Americans and "whites" (2012: 64). He argues that "Power processes that exist on reservations are overlooked and the dynamics of political change go unaccounted for and part of native lives remains peculiarly caged" (2012: 65). It is thus important to acknowledge that certain disciplinary "cages" and informal taboos shape knowledge production.

2. In Abidjan, for example, Sasha Newell (2012: 65) noted that his Ivorian friends "were loath to admit" to work at low-level, part-time jobs, which was "so demeaning that it had to be avoided or hidden from one's community." In postwar Inhambane, most young residents have "more to hide than to display, whether it is what they did—such as their involvement in criminal and sexual activities—or what they lacked—that they slept on the floor for want of a bed, skipped meals, or wore trousers with missing buttons and a broken zipper" (Archambault 2017: 60).

3. For example, in Kinshasa, a common saying is that "not all truth needs to be told."

4. "How African Governments Undermine the Use of Encryption." 2021. CIPESA, October. Retrieved 5 January 2022 from https://cipesa.org/?wpfb_dl=477.

5. This category of "inside meanings" did not appear with digitalization, of course; Aboriginal bark painting harbors similar inside and outside meanings. "Inside meanings" then refer to "the dimensions of stories and images that cannot be made public—or can only be revealed through ceremony." Visual effects may be sprinkled on digital photographs in order to suggest a "shimmering effect," a sense of the emergence of the ancestral land. On the glimmering surface of the screen, discursive and affective realms bring together "personal biographies, ancestral stories, and family" (Deger 2016: 125). Similarly, "deep or inside" ancestral knowledge will not easily be conveyed in the public arena, and it may be protected by sorcery or other means.

References

Abu-Lughod, Lila. 1993. *Writing Women's Worlds: Bedouin Stories*. Berkeley: University of California Press.

Archambault, Julie Soleil. 2017. *Mobile Secrets: Youth, Intimacy, and the Politics of Pretense in Mozambique*. Chicago: Chicago University Press.

Babel, Anna. 2018. "The Invisible Walls of the Whisper Network." *Anthropology News*, 10 May 2018. https://doi.org/10.1111/AN.859.

Barber, Karin. 1987. "Popular Arts in Africa." *African Studies Review* 30(3): 1–78.

Bernal, Victoria. 2020. "The Aesthetics of Cyber Insecurity: Displaying the Digital in Three American Museum Exhibits." In *Futureproof: Security Aesthetics and the Management of Life*, ed. Asher Ghertner, Daniel Goldstein, and Hudson McFann, 33–62. Durham, NC: Duke University Press.

———. 2021. "The Cultural Construction of Cybersecurity: Digital Threats and Dangerous Rhetoric." *Anthropological Quarterly* 94(4): 611–38.

Beshiri, Arber, and Asim Susuri. 2019. "Dark Web and Its Impact in Online Anonymity and Privacy: A Critical Analysis and Review." *Journal of Computer and Communications* 7(3): 30–43.

Chandra, Giti, and Irma Erlingsdóttir, ed. 2020. *The Routledge Handbook of the Politics of the #Metoo Movement*. Abigdon: Routledge.

Clifford, James and George Marcus. 1986. *Writing Culture: The Poetics and Politics of Ethnography*. Berkeley: University of California Press.

Coleman, Gabriella. 2014. *Hacker, Hoaxer, Whistleblower, Spy: The Many Faces of Anonymous*. New York: Verso Books.

Comaroff, Jean, and John Comaroff. 1999. "Occult Economies and the Violence of Abstraction: Notes from the South African Postcolony." *American Ethnologist* 26(2): 279–303.

Cooper, Elizabeth, and David Pratten, ed. 2015. *Ethnographies of Uncertainty in Africa*. Basingstoke: Palgrave McMillan.

Couldry, Nick, and Ulises Mejias. 2019. "Data Colonialism: Rethinking Big Data's Relation to Contemporary Subject." *Television & New Media* 20(4): 336–49.

Deger, Jennifer. 2016. "Thick Photography." *Journal of Material Culture* 21(1): 111–32.

Drakulich, Kevin, Kevin Wozniak, John Hagan, and Devon Johnson. 2020. "Race and Policing in the 2016 Presidential Election: Black Lives Matter, the Police, and Dog Whistle Politics." *Criminology* 58(2): 370–402.

Ferme, Marian. 2001. *The Underneath of Things: Violence, History, and the Everyday in Sierra Leone*. Berkeley: University of California Press.

Geertz, Clifford. 1973. *The Interpretation of Cultures: Selected Essays*. New York: Basic Books.

Groos, Jan. 2020. "Crypto Politics: Notes on Sociotechnical Imaginaries of Governance in Blockchain Based Technologies." In *Data Loam: Sometimes Hard, Usually Soft; The Future of Knowledge Systems*, ed. Johnny Golding, Martin Reinhart, and Mattia Paganelli, 148–70. Berlin: De Gruyter.

Hejoaka, Fabienne. 2009. "Care and Secrecy: Being a Mother of Children Living with HIV in Burkina Faso." *Social Science and Medicine* 69: 869–76.

Hellegren, Isadora. 2017. "A History of Crypto-Discourse: Encryption as a Site of Struggles to Define Internet Freedom." *Internet Histories* 1(4): 285–311.

Herzfeld, Michael. 2009. "The Performance of Secrecy: Domesticity and Privacy in Public Spaces." *Semiotica* 175: 135–62.

Hinds, Joanne, Emma Williams, and Adam Joinson. 2020. "'It Wouldn't Happen to Me': Privacy Concerns and Perspectives Following the Cambridge Analytica Scandal." *International Journal of Human-Computer Studies* 143: 102498.

Hintz, A., Lina Dencik, and Karin Wahl-Jorgensen. 2017. "Digital Citizenship and Surveillance Society: Introduction." *International Journal of Communication* 11: 731–39.

Jarvis, Craig. 2020. *Crypto Wars: The Fight for Privacy in the Digital Age; A Political History of Digital Encryption*. Boca Raton, FL: CRC Press.

Jones, Graham. 2014. "Secrecy." *Annual Review of Anthropology* 43: 53–69.

Kabir, Ananya. 2014. "Cryptopolitics and Cyberpoetics: Facebook Pages as Memory Portals." *MLA Profession.* Retrieved 13 January 2023 from https://profession.mla.org/cryptopolitics-and-cyberpoetics-facebook-pages-as-memory-portals/.

Kitanaka, Junko. 2015. "The Rebirth of Secrets and the New Care of the Self in Depressed Japan." *Current Anthropology* 56(S12): S251–62.

Mackworth-Young, Constance, Virginia Bond, and Alison Wringe. 2020. "Secrets and Silence: Agency of Young Women Managing HIV Disclosure." *Medical Anthropology* 39(8): 720–34.

Manderson, Lenore, Mark Davis, Chip Colwell, and Tanja Ahlin. 2015. "On Secrecy, Disclosure, the Public, and the Private in Anthropology." *Current Anthropology* 56(S12): S183–S190.

Meyer, Birgit. 2015. *Sensational Movies: Videos, Vision, and Christianity in Ghana.* Berkeley: University of California Press.

Miller, Daniel, Elisabetta Costa, Nell Haynes, Tom McDonald, Razvan Nicolescu, Jolynna Sinanan, Juliano Spyer, Shriram Venkatraman, and Xinyuan Wang. 2016. *How the World Changed Social Media.* London: UCL Press.

Monsees, Linda. 2019. *Crypto-politics: Encryption and Democratic Practices in the Digital Era.* London: Routledge.

Newell, Sasha. 2012. *The Modernity Bluff: Crime, Consumption, and Citizenship in Côte d'Ivoire.* Chicago: Chicago University Press.

Nuttall, Sarah, and Achille Mbembe. 2015. "Secrecy's Softwares." *Current Anthropology* 56(S12): S317–S324.

Obadare, Ebenezer. 2016. *Humor, Silence, and Civil Society in Nigeria.* Rochester, NY: University of Rochester Press.

Orr, Raymond. 2012 "Notes from the Field: Regarding Iron Cages; Crypto-Politics and the Hidden Conflicts of American Indians." *Arizona Anthropologist* 22: 59–65.

Pype, Katrien. 2011. "Confession-cum-Deliverance: In/Dividuality of the Subject among Kinshasa's Born-Again Christians." *Journal of Religion in Africa* 41(3): 280–310.

———. 2012. *The Making of the Pentecostal Melodrama: Religion, Media, and Gender in Kinshasa.* Oxford: Berghahn Books.

Rajewsky, Irina. O., 2005. Intermediality, intertextuality, and remediation: A literary perspective on intermediality. *intermédialités*, (6), pp.43-64.

Rhine, Kathryn. 2014. "HIV, Embodied Secrets, and Intimate Labour in Northern Nigeria." *Ethnos* 79(5): 699–718.

Rigby, T. H. 1965. "Cryptopolitics." In *The State of Soviet Studies,* ed. Walter Laqueur and Leopold Labedz. Cambridge, MA: MIT Press.

Rodima-Taylor, Daivi. 2021. "Digitalizing Land Administration: The Geographies and Temporalities of Infrastructural Promise." *Geoforum* 122: 140–51.

Rodima-Taylor, Daivi, and William Grimes. 2019. "International Remittance Rails as Infrastructures: Embeddedness, Innovation and Financial Access in Developing Economies." *Review of International Political Economy* 26(5): 839–62.

Scott, James. 1985. *Weapons of the Weak: Everyday Forms of Resistance.* New Haven, CT: Yale University Press.

———. 1990. *Domination and the Arts of Resistance: Hidden Transcripts.* New Haven, CT: Yale University Press.

Simmel, George. 1906. "The Sociology of Secrecy and of Secret Societies." *American Journal of Sociology* 11(4): 441–98.

Taussig, Michael. 1999. *Defacement: Public Secrecy and the Labor of the Negative.* Stanford, CA: Stanford University Press.

Weiman, Gabriel and Ari Ben Am. 2020. "Digital Dog Whistles: The New Online Language of Extremism." *International Journal of Security Studies* 2(1): 4.

West, Harry G., and Todd Sanders, ed. 2003. *Transparency and Conspiracy: Ethnographies of Suspicion in the New World Order.* Durham, NC: Duke University Press.

White, B. W. 2007. "La quête du lupemba: rumeurs, réussite et malheur en République démocratique du Congo" [The quest for lupemba: rumors, success and misfortune in the Democratic Republic of Congo]. *Sociologie et sociétés* 39(2): 61–77.

White, Louise. 2000. *Speaking with Vampires: Rumor and History in Colonial Africa.* Berkeley: University of California Press.

Zuboff, Shoshana. 2019. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power.* New York: PublicAffairs.