Dangerous Networks
Internet Regulations as Racial Border Control in Italy

Camilla A. Hawthorne

How does a particular technology enable certain power-laden practices of "racializing surveillance" (Browne 2012), practices that also coincide with national borders?[1] Following the 2004 train bombings in Madrid and the 2005 attacks on London's public transportation system, the Italian government quickly enacted the strictest Internet regulations in the European Union. Law No. 155/2005, popularly known as the Pisanu Decree, was intended as an antiterrorism package that would protect Italian citizens from the threat of "Internet users who have been sensitized by Al Qaeda" ("Informativa Del Governo" 2005). The Pisanu Decree included a slate of new surveillance procedures targeting Internet cafés—businesses that in Italy are largely immigrant owned, operated, and frequented. The Pisanu regulations required the mandatory collection of identification documents for all Internet café users, as well as their web browsing histories. At the same time, the physical space of the Internet café emerged as a regular target for police inspections and raids against immigrants of color and Muslims. This chapter explores the lifespan of the Pisanu Decree's Internet café regulations (2005–12) to argue that sociotechnical imaginaries (Jasanoff and Kim 2009) and governmental practices of immigration control are always co-constructed and, in the case of the Italy, generated new practices of border drawing and racial classification that worked through the *placefulness* of Internet access. This networked surveillance was profoundly spatial, filtering the "metadata" of an individual's movements, associations, and situated technological habits through stereotypical understandings of Muslim culture in order to constitute a new, identifiable racial subject—the radicalized, male Muslim Internet user lurking within the nation's borders.

Early theorists of cybercultures portrayed the Internet as a deterritorialized "space of flows" (Castells 2000; cf. Shklovski et al. 2013, 12) with the power to simultaneously render borders insignificant, challenge the authority of centralized nation-states, and eliminate both identity politics and body-based forms of prejudice (Turner 2006). The idea of the "borderless" Internet was dealt a significant blow by the rise of Web 2.0 around 2005, as well as the 2013 revelations of NSA

telecommunication surveillance through PRISM and MUSCULAR (the latter in collaboration with the British Government Communications Headquarters). While extensive literature exists on the use of biometric technologies for border securitization (Magnet 2011), however, the deployment of Internet regulations and surveillance to reinforce borders and control immigrant populations remains an underexplored topic. In the post-9/11 era, governments around the world have increasingly enrolled the Internet into their border control efforts through surveillance strategies that are folded into national security and antiterrorism programs that disproportionately target communities of color. The notion of the "splinternet" (Thompson 2010; Ananthaswamy 2011; Malcomson 2016), a term coined to describe the global instantiation of multiple, stratified Internets as a result of paid "walled gardens" and government firewalls, can thus be applied here to refer to the way in which the Internet is experienced as freedom for some and surveillance for others.

Just as the Internet is not frictionless, the Internet is not raceless; we must therefore continue to heed Donna Haraway's provocation in the "Cyborg Manifesto" (1991, 165) to take seriously the "rearrangements of race, sex, and class rooted in high-tech facilitated social relations." Central to the argument of this chapter is an understanding of race itself as a sociotechnical system—an "arrangement of humans, technologies, architectures, spaces, and policy regimes" that encompass "the biological, the sociological, the political, and the technical" (Forlano and Jungnickel 2015). Thus, race is not a stable category but rather articulates with human and nonhuman actors, policy regimes, and historical processes to generate new and often contradictory meanings in the present. And just as the theoretical tools of STS can help to open the "black box" of race, they can also uncover the embedded assumptions, imaginaries, practices, infrastructure, and relationships that are too often glossed as "the digital." If race is a sociotechnical rather than a biological phenomenon, then in the digital age technologically mediated social networks are the raw materials for the construction of racial subjects.

In the case of Italy, the government's sociotechnical imaginary of the Internet as an unruly, dangerous space of cyber-networking facilitated new forms of capillary control, surveillance, and territorialization. The Pisanu Decree operated through the temporal and spatial expansion of the border through networked surveillance practices, as well as the aggregation, analysis, and reassembly of web traffic data linked to nonvirtual sites such as urban Internet cafés in immigrant enclaves. By reworking older forms of racial boundary drawing in Italy, these everyday "border controls" made it possible for the state to identify threatening subjects through the isolation of specific, suspicious technological spaces, practices, and associations.

This chapter begins with a brief overview of Italy's transition from a country of emigration to a country of immigration, with a focus on the politics of difference and the criminalization of migration. I then turn to a review of theories pertaining to race and the Internet, as well as insights from postcolonial STS about the relationship between race, technology, and Western ideas of civilizational progress. The third section of the chapter analyzes the enactment, enforcement, and limitations of the Pisanu Decree through legislative reports, government documents, and popular media. I conclude with an analysis of the politics of digital circulation in Italy and the distinctiveness of racial profiling through Internet surveillance as opposed to systems such as biometric bordering.

Context: Immigration and Racism in Contemporary Italy

Historically, Italy was a country of mass emigration. Analysts have attributed Italy's transformation into a country of immigration in the 1980s to a variety of factors, with the result that by the end of the 1990s Italy's population began to represent a new plurality of national groups (Merrill 2006). The 2005 Pisanu Decree must be situated within the context of a much broader shift from laissez-faire to highly restrictive Italian immigration policies that also involved Italy's participation in the Schengen Agreement and the border regimes of Fortress Europe, Silvio Berlusconi's alliance with the far-right Northern League, and a post-9/11 emphasis on securitization. At the heart of the debates surrounding immigration to Italy is a profound ambivalence about Italy's position as a site of postcolonial immigration. Despite the fact that Muslims represent less than two percent of Italy's population, Islam in particular—as the second most widely practiced religion in Italy—has catalyzed a widespread moral panic about religious and cultural difference. Thus, immigration law, citizenship policies, the interiorization of the border through surveillance, and the proliferation of informal multiculturalisms in Italy can all be understood as efforts to manage internal difference in Italy.

It is also important to note that despite a long and troubled history of race thinking and the use of race as an organizing principle for the Italian nation, "race" as a descriptive or analytical category was disavowed in post–World War II Italy (Mellino 2012). Use of the word *razza* (race) remains taboo due to its association with fascism; instead, *etnia* (ethnicity) is commonly deployed to mark human groups. The discursive vacuum surrounding race in Italy has not repressed discussions about difference and national belonging, but instead has incited multiple state and non-state sources to engage different genealogies of Italianness and generate alternative modes of essentialization. These include, but are not limited to, geography, language, religion, and cultural inheritance. Indeed, as Stoler ([2002] 2010, 144) contends (via Foucault's refusal to conflate "race" with the biological), racisms gain their force from the "internal malleability assigned to the changing features of racial essence." In the context of digital surveillance, categories such as religion are fused to associations between technological practices and technologically mediated social relations to fix individuals as classifiable racial subjects. An STS-inflected understanding of race as a sociotechnical practice can therefore reveal the ways in which racial meanings are rearticulated with the digital even when the word "race" is not uttered.

STS and the Politics of Race on/and the Internet

The enactment of the Pisanu Decree's antiterrorism package suggests that deployments of technology cannot be analyzed separately from questions of difference, and that the meanings of "race" are themselves actively transformed by technologies. An understanding of Internet surveillance as co-constitutive of racial categorization requires a different theoretical genealogy of the relationship between race and the Internet. In other words, it requires shifting from an understanding of the Internet as merely a tool that can be used for racist purposes (for instance, by controlling circulation and access to information for specific groups, or spreading harmful stereotypes) to one in which the Internet, as a sociotechnical space of practices, is entangled with ever-evolving articulations of racism and race (for instance,

through menu designs that unintentionally reify bounded racial groups, or surveillance algorithms that essentialize and criminalize individuals based on the geographies of their digital webs of association).[2] This is of course *not* to suggest that the Internet, as a sort of "sentient" agent, deterministically produces race out of whole cloth, creating racisms where they did not previously exist.

It is important to note that scholars of postcolonial and feminist science and technology studies have long pointed to the inextricable relationship between science, technology, racism, and modernity (Haraway 1989; Prakash 1999; Drayton 2000; Mitchell 2002; Phillip 2003). Their insights are relevant to any discussion of "racial formation" (Omi and Winant 1986) and the Internet. Within the context of European colonial expansion, technological difference was coded as racial difference and inferiority, and thus served as a justification—vis-à-vis notions of "civilizing missions"—for globe-spanning European imperial entanglements. Colonized natives, for failing to rise above the natural world with the help of domesticating technologies, were bounded as part of nature, which itself was constructed as a separate object for technological intervention by rational, detached experts.

Following the rupture of the dotcom bubble in 2000, however, a new body of scholarship emerged from the fields of new media and science and technology studies that critically reexamined some of the initial emancipatory promises and "founding fictions" (Nelson 2002, 1) of the Internet. The gleeful utopianism of early Silicon Valley cyberculture, as chronicled by Fred Turner (2006), was characterized by a conviction that virtual communities had the power to render categories such as race and gender obsolete and foster the elaboration of associational forms that were no longer bounded by spatial proximity. One important line of inquiry in the post-2000 literature focused specifically on challenging the claim that race and racism would cease to exist online. Key theorists of race and the Internet (Nakamura 2002, 2007; Nelson 2002; Chun 2006; Landzelius 2006; McGahan 2008; McLelland 2008; Daniels 2009; Everett 2009) argued that, in fact, race had actually *proliferated* on the Internet (Chun 2006) in the forms of racial identity tourism, visual and textual representations of race in community forums and games, and online white supremacist outposts. Prior to this work, most discussions of race on the Internet focused on "digital divides," a concept that scholars such as Nakamura (2002, 2007), Chun (2006), and Everett (2009) have critiqued in part for failing to capture the creative cultural productivity of minorities on the Internet. Attempts to revise this portrayal of minority groups as technologically lacking have taken the form of counternarratives that emphasize Black "technolust" (Everett 2009), emancipatory Afrofutures (Dery 1994), or digital innovation. Such redemptive stories of minoritarian cybercultures, however, are now being superseded by cautionary narratives of racist stereotyping, bullying, and surveillance online.

Key to this literature is the suggestion that digital disembodiment does not necessarily bring with it liberation from oppressive categories of race, gender, sex, or nation (Nguyen 2003). Instead, the Internet actually "propagates, disseminates, and commodifies" images of race (Nakamura 2002, 3). Reductive representations of race on the Internet serve to anchor or stabilize cyberspace precisely because it is imagined as a medium that severs the link between intelligible material bodies and representation; as Nakamura (2002, 5) writes, these "cybertypes" (online racial or ethnic stereotypes) "both stem from a common cultural logic and seek to redress anxieties about the ways that computer-enabled communication can challenge these old logics." The paranoia produced by the invisibility of technology is expressed as discourses of regulation and control that, in the post-9/11 period,

now focus on dangerous people—e.g., terrorists—as opposed to dangerous content—e.g., pornography (Chun 2006). In other words, the Internet can be simultaneously reified as a postspatial, postracial utopia of unrestricted freedom and as a dangerous, unruly space that must be secured through the mobilization and reinscription of race and racial categories—a phenomenon Chun (2006) calls "control-freedom."

Implicit in these arguments is that centering the materiality and spatiality of the Internet can also reveal the reproduction of racisms and race online. Contrary to outdated predictions of "global villages" (McLuhan ([1962] 2011) and interactive communities based "not on common location but *common interest*" (Licklider and Taylor [1968] 1990, 3), Internet use is in fact characterized by experiences of friction (Tsing 2005), unevenness (Kraemer 2013), and boundaries (Shklovski et al. 2013)—including national boundaries. After all, the persistent influence of quotidian "offline" factors such as time zones (Boellstorff et al. 2012), along with political and infrastructural factors such as Internet censorship, surveillance, and bandwidth restrictions, serve as an important reminder that the Internet is not an abstract, intangible medium but is instead shaped by material realities and physical, embodied practices (see Nemer and Chirumamilla, this volume).

Race on the Internet can be thus understood as both restrictive—performing boundary work to militate against forms of cultural hybridity that do not conform to narrow, cosmetic multiculturalisms (Nakamura 2002, 20–21)—and generative of new modes of representing racial bodies (Nakamura 2007, 13). In addition, race itself is constitutive of the Internet. For example, race and gender are integral to hardware production and communication service provision (see Poster, this volume)—the individuals who assemble circuit boards and other electronic components, or who work in call centers, are largely women and/or of Asian heritage (Chun 2006, 72–73). In addition, race (or its disavowal) was central to the conception of cyberspace as utopian (Chun 2006, 129) and populated by unmarked "virtual homesteaders" (Rheingold 1993).

To conclude, the relationship between race and technology is structured in dominance, and can be expressed in three ways. First, technologies enable new forms of racialization, or racial categorization and boundary drawing. Second, the concept of technology is itself racial, fundamentally intertwined with Enlightenment-era scientific racisms that link the technological subjugation of the natural world with modernity, civilization, and progress (Adas 1990). Third, race can also be understood as a technology, a "levered mechanism" (Coleman 2009, 178) that "creates parallel social universes and premature death" (Benjamin 2016). But how are we to think specifically about the interplay of race and technology in relation to emerging border regimes? The case of the Pisanu Decree suggests that sociotechnical imaginaries of the Internet and Internet users can render technology as both *marker of* and *tool for* racial classification. The identification of certain forms and physical spaces of Internet activity can be used to isolate Others who are believed to threaten the integrity of the national body.

Securing Cyberspace: The Pisanu Decree and Internet Surveillance

Following a string of terrorist attacks in Madrid (2004) and London (2005), the Italian legislature moved quickly to enact a new set of national antiterrorism policies. The speed and near-unanimity with which this legislation was approved were remarkable, given the notoriously glacial pace of Italian government proceedings.

Law No. 155/2005 ("Urgent Measures for Combatting International Terrorism," also known as the Pisanu Decree) passed on July 31, 2005 and contained a series of new procedures governing residency permits, immigrant expulsion, telecommunication surveillance, and flight school administration (Conversione in Legge 2005). Article 7 of the law focused exclusively on public Internet use and included the following key provisions:[3]

1. Anyone who opens a new public Wi-Fi hotspot or public space with terminals for electronic communication (i.e., an Internet café) must first apply for a license from the local police headquarters. A license is not necessary for operators of public pay phones with only voice telephony services. This license is dependent upon the establishment having put in place appropriate data monitoring and retention systems; license applicants are also required to submit detailed information about their businesses, including floor plans (Hooper 2005).
2. The owner or operator of an Internet café must monitor the activities of customers and archive their data for at least six months—this includes documenting what computers they use, recording their log-in and log-out times as well as when they enter and exit the premises, and purchasing tracking software that saves a list of all sites visited (Celeste 2005). The web browsing logs must be submitted periodically to local police headquarters.
3. The owner or operator of an Internet café must record customers' personal data by photocopying an identity document such as a passport.

At this time, Italy already followed the 2002 amendment to the European Union Directive on Privacy. Article 15 permits Internet service providers to temporarily retain records of user activity, which can then be made available to law enforcement for the purpose of safeguarding "national security . . . defence, public security, and the prevention, investigation, detection, and prosecution of criminal offenses" (OpenNet Initiative 2010).[4] While the earlier 1997 EU privacy directive had required ISPs to erase customers' communication traffic data (Levi and Wall 2004, 203), the 2002 amendment allowed European Union member states to selectively restrict Internet users' right to privacy in the context of state security (European Parliament and Council 2002)—somewhat like the infamous USA PATRIOT Act 2001. In Italy, ISPs were required to cooperate with police and courts during investigations, but did not retain any online activity data except for the details of Internet payments for up to six months (Reporters without Borders 2004).

Although several European countries introduced new security measures after the London bombings (BBC 2005a), the Pisanu Decree established Italy as the only country in the European Union to require the presentation of identity documents at Internet cafés (Switzerland, which is not an EU member, did require Internet café customers to show ID). Some left-leaning politicians concerned with the suspension of individual rights to privacy contested these provisions; however, their reservations were ultimately outweighed by a more dominant preoccupation with terrorism and national security. The Pisanu Decree ultimately passed both chambers of the Italian Parliament with sweeping majorities.

Accordingly, the Pisanu Decree also marked the beginning of a period of intensified Internet surveillance in Italy, under the auspices of national security. Internet privacy advocates have previously suggested that the heavy-handedness of the Pisanu Decree and other attempts at Internet regulations in Italy can be attributed

to the Italian government's lack of understanding of the Internet and privacy issues (Pavis 2000; OpenNet Initiative 2010); indeed, Internet penetration rates in Italy have consistently lagged behind those of most other European countries. The post-2005 move toward greater surveillance of the Internet and Internet access points in Italy can be more accurately described, however, as an imperfect attempt to resolve the inherent tensions between the ideal of Internet freedom and a concern with online terrorist networks. By focusing on specific *sites* of Internet use, which were in turn connected to specific *types* of Internet users, the Italian state could respond to growing popular and international calls for antiterrorist Internet surveillance in the wake of Madrid and London. A preoccupation in Italy with the dangerous connections that could be formed through the Internet, however, can be traced at least to 2004—in the wake of global post-9/11 surveillance and securitization efforts (Levi and Wall 2004). That year, the Ministry of the Interior reported to the Italian Parliament that "the use of telecommunication networks by fundamentalist groups represents an aspect of intense interest, as the Internet has now taken on the form of an interactive mass medium, whereas before the network was used as a means of internal communication among small groups with strictly operational needs" (Terrorismo Ed Eversione 2004, 17).[5] In this report, the Internet was figured as a sprawling network that facilitates unlimited communication and interaction among individuals who are not necessarily known to each other—a departure from a supposed earlier, less threatening iteration of Internet networking for benign purposes.

A 2010 Ministry of the Interior document titled "Security, Immigration, and Asylum" reflected the operationalization of this concern with jihadist networks on the Internet. According to the document, "Specific attention has been dedicated to the fight against radicalization and recruitment, starting with the monitoring of the Internet" (Ministero dell'Interno 2010, 11). In 2012, the Ministry of Justice published a report about Islamic radicalization in the penitentiary system. Although the report ostensibly addressed proselytization in Italian prisons, the authors devoted significant space to the dangers of the Internet:

> The development of the information society, in fact, has not escaped the Islamic world and the potential offered by new technologies (especially the Internet) constitutes one of the principle vehicles for the diffusion of ideologies, allowing something born at the local level to transform into something global. . . . The shared function of these various sites is that they sustain the jihadist infrastructure through the distribution of communications, secret messages, and propaganda materials, and we cannot forget the important role that they play in the recruitment of potential jihadist candidates. In fact, the main concern resides in the fact that the Internet has become a virtual training field. (Ministero della Giustizia 2012, 27)

As a result, the authors recommended the monitoring of "Internet networks" with a focus on jihadist sites and, in particular, discussion forms, along with the control of Internet cafés and other sites "frequented by radical elements" (Ministero della Giustizia 2012, 31). By incorporating a discussion of the Internet into a report about the Italian penitentiary system, the authors suggested that an unmonitored Internet has the potential to penetrate and undermine one of the most robust symbols of the state's power to discipline the population within its borders: the prison.

The concept of sociotechnical imaginaries is useful for understanding how the Internet was directly enrolled into Italy's national security and border control efforts in 2005. According to Jasanoff and Kim (2009, 120), sociotechnical imaginaries are "collectively imagined forms of social life and social order reflected in the design and fulfillment of nation-specific science and/or technological projects." Sociotechnical imaginaries prescribe "futures that ought to be attained" (120), but also warn against "risks or hazards" (123). Unlike popular media tropes, however, sociotechnical imaginaries are closely associated with the flexing of state power and the enactment of national policies (123).

Sociotechnical imaginaries move discussions of technology away from technologically determinist framings in which a technical system is locked in to a predetermined set of politics, policies, and social arrangements. Unlike Winner (1989), who suggests that particular technological artifacts are compatible with certain social and political orders, Jasanoff and Kim suggest that sociotechnical imaginaries and social orders or policies produce one another in a dynamic relationship that varies over both space and time. This insight is particularly valuable when discussing a technology such as the Internet. The openness of the Internet, as it is popularly understood, is simultaneously perceived as both liberating and threatening. In addition, the Internet as a decentralized network (admittedly, an oversimplification of its material infrastructure) is conducive both to freedom and to new forms of surveillance or "networked authoritarianism" (Pearce and Kendzior 2012). Italian policy makers' engagements with the Internet as a space of dangerous, unrestrained transnational networking that cannot be contained by national borders—influenced not only by post-9/11 terrorist attacks but also by Italy's own experiences with domestic terrorism by the Red Brigades and far-right groups during the Years of Lead and the vast criminal networks of the mafia—can thus be understood as a form of sociotechnical imagination.

Yet, as Benjamin (2016) notes, Jasanoff and Kim's formulation also acknowledges the coexistence of multiple imaginaries of a technology within a particular national space. These imaginaries can be deployed toward different ends and in relation to different populations. The Italian sociotechnical imaginary of the Internet is not unified, but rather incorporates racial distinctions between different kinds of Internet use: public versus private, individual versus communal, European versus non-European, cosmopolitan versus ethnically particularistic.

The debates in the Italian legislature surrounding the passage of the Pisanu Decree reflected a conflation of concerns about security and radical Islam, fears that were refracted through popular imaginaries of the Internet. Indeed, it was quite common during this time to see salacious news stories circulating in the Italian media that explicitly linked Internet use, the threat of terrorism, and undocumented immigration. The passage of the security package was justified with references to the London bombings and the fact that Internet surveillance and the policing of Internet cafés were used by police forces in both Italy and the United Kingdom to identify and locate suspected terrorists. In particular, the arrest in Rome of Hussein Oman (also known as Hamdi Isaac)—one of the men behind the London bombings who also supposedly communicated with his relatives in Italy over the Internet (BBC 2005b)—framed discussions about the securitization of the Internet and Internet cafés. Still, despite several vague terrorist threats against Italy due to the country's involvement in the Iraq War, Beppe Pisanu (then minister of the interior and namesake of Law No. 155/2005) admitted during discussions of the antiterrorism package that there was no specific evidence of an impending

attack (BBC 2005a). According to Carlo Taormina, a member of the Chamber of Deputies with Silvio Berlusconi's conservative Forza Italia party, however, "The tools of investigation, which this decree will strengthen, enabled the effective identification of the person responsible for the failed attack on the London Underground on 21 July 2005. . . . It was possible to achieve the identification of the person responsible through the utilization of telephone tracking and through the identification of the people who provided the terrorist with logistical support—the operator of an Internet café, which will be subject to more restrictive control thanks to the application of the measures in the decree under discussion" (Decreto-legge 144/05 2005). During the debate, other legislators expressed concern that the Internet makes a wide spectrum of information about the preparation and use of explosive materials, firearms, and other types of weapons easily accessible. These anxieties about the information that can be accessed through the unrestricted networks of the Internet resurfaced in a December 2005 review about the first months of the Pisanu Decree's implementation. During this special parliamentary session, several legislators and government officials suggested that jihadist websites hosted in the Middle East could pose serious, material threats to the Italian social and political order. Pisanu reminded parliamentarians about online jihadist media outlets such as the Global Islamic Media Front:

> I remember as well that last November the Global Islamic Media Front, a promoter of what is considered "news" from Al Qaeda, distributed over the Internet a video reaffirming the strategy of the terrorist organization: recruitment, training, and encouragement of the mujahedeen over the web; promotion of jihadist media to intimidate the "crusaders"; and celebration of Al Qaeda in Mesopotamia as an example for all of the other armed movements. Subsequently, on 24 November, the same organization distributed a threat against the President of the Council of Ministers and the Italian people. In general, we can consider these various threats against our country as the work of Internet users who have been sensitized by Al Qaeda, who pose a very high risk, and play on their knowledge of current Italian politics. ("Informativa Del Governo" 2005)

Pisanu describes the Internet as a dangerous, decentralized transnational network for the dissemination of both propaganda and violence. In his statement, the primary danger to the Italian people is the Internet as an "*open* university in terrorism" (Chun 2010, 343), not terrorism itself. Notice, for instance, that he characterizes these threats against the Italian people as the work of "Internet users," *not* terrorists, who have been radicalized by Al Qaeda through their online encounters with jihadist websites. These Internet users, whose physical location is unspecified and uncertain, are also able to infiltrate the Italian political system and then use this information to generate threats to the country's national security.

The Internet Café as Zone of Alterity

In the implementation of the Pisanu Decree, Internet cafés became material spaces of intervention into the supposedly dangerous, immaterial networks of the Internet. In order to grasp the significance of the Internet café, it is important to first situate these spaces within the broader context of immigration to Italy. Internet

cafés are popularly imagined as immigrant spaces, even though they also cater to tourists. They are usually clustered in areas with large immigrant populations, such as the neighborhood behind Rome's main Termini train station, and often serve as meeting places for "a community of newcomers" (Carter 2013, 203). Over the past 20 years, a growing need for money transfer centers (which are usually colocated with Internet cafés) for diasporic remittances, along with restrictive business and employment regulations that also favor Italian citizens, have created a niche for migrant self-employment through Internet cafés. A 2012 report found, for instance, that almost 94% of the Internet cafés in Rome are operated by foreigners (*Yalla Italia* 2012). While Internet cafés are themselves not highly lucrative enterprises, a factor that explains the dearth of Italian-owned Internet cafés, immigrant families often manage other businesses such as restaurants or shops that help to distribute costs, profits, and risk among different family ventures.

The association of Internet cafés with immigrants in Italy has been a major source of tension and fear for many "native" Italians. In the Reggio Emilia province, for instance, Forza Italia leader Claudio Guidetti remarked that Internet cafés and call centers are frequented mostly by "undocumented or irregular immigrants or those dedicated to terrorism" (Provincia Di Reggio Emilia 2006). In 2009, journalist Tom Kington interviewed an anti-immigrant protester in Tuscany who lamented that not just the kebab shops but also the call centers and Internet cafés were all "managed by foreigners" (Kington 2009).

The association of Internet cafés with immigrants is also closely linked to the relationship between software and modernity (Chun 2010). The computer and Internet access, like the plow for an earlier generation of anthropologists (see Goody [1971] 1980), are commonly used as markers of civilization and modernity. It is for this reason, as Chun (2006) argues, that "digital divide" rhetorics have troublingly colonial undertones. A conception of "bridging the digital divide" solely in terms of Internet access or laptop usage, for instance, would create "'junior users' not unlike 'colonized' subjects who were structurally dependent on knowledge from the motherland" (Chun 2006, 152; see also Burrell 2012). Importantly, however, computer usage must be linked to *personal* ownership (tied to Lockean understandings of individual property rights) if one is to be situated on the "correct" side of this digital divide (Chun 2010; see also Chan, this volume).

Viewed in this context, the Internet café stands as a marker of an uncivilized, premodern form of communal computer use. The Internet café is not just an "immigrant space," then; it is also a zone of technological Otherness and backwardness. This distinction between personal and communal ownership of technology articulates with Italian parliamentarians' association of Islam with collectivism rather than liberal individualism. In a Chamber of Deputies hearing, Umberto Ranieri of the social democratic Democratici di Sinistra party observed,

> This is a complex question: immigrants in the West express a religious question that serves to reinforce an identity put in crisis by the disorienting experience of immigration and that directs them to the network of mosques and Islamic associations. However, even on this point it is important to be careful: the association of Islam with a total ideology, a system that does not accept distinctions between religion and politics, is not shared by the majority of Muslim immigrants. All of the experts say it, the move to the West changes the relationship of Muslims with their religion and signals a progressive individualization. (Disegno di Legge di Conversione 2005)

Islam in this statement is associated with strong cultural ties—and potentially dangerous religious networks—that subsume the individual beneath a larger set of community obligations. This is, of course, a classically Orientalist portrayal of the Muslim world (Said [1978] 2014). According to Ranieri's "experts," however, migration to the West leads to a teleological process of individualization in which the individual Muslim immigrant is able to extricate herself or himself from these overbearing, non-Western cultural networks. It is no surprise, then, that Internet cafés, which allow Muslim immigrants to potentially access jihadist websites, are associated with this sort of dangerous collectivism. Internet cafés, as spaces of communal technology use, can reverse the modernization process catalyzed by the experience of migration to Italy and immersion in "Western" or "European" society. In other words, Internet cafés are spaces that enable new kinds of social relations that Italian policy makers perceive as highly threatening to Italian national security and social order.

Once enacted, the Pisanu Decree had a disproportionate impact on immigrant communities in Italy, and particularly on undocumented immigrants. A Bangladeshi immigrant and Internet café owner interviewed shortly after the law passed lamented, for instance, that he had no clients left (Sanminiatelli 2005). This reduction in clientele has been largely attributed to the law's ID registration requirement. Several cafés whose customers included undocumented immigrants turned a blind eye to this provision; in fact, one sociologist described the law as "useless" because customers intent on using Internet cafés could simply present false identification documents in order to skirt the regulations (Sanminiatelli 2005). Still, the ID requirement had a significant chilling effect on Internet café use among those immigrants, who chose to employ analog "privacy enhancing strategies" (Levi and Wall 2004, 210) to displace the impact of surveillance, such as avoiding Internet cafés altogether. In addition, the labyrinthine requirements for Internet café registration discouraged many entrepreneurially minded immigrants from opening new businesses.

In addition to the Pisanu Decree's requirement of ID collection and data tracking in Internet cafés, the Italian police also regularly targeted Internet cafés as sites for inspections and immigration raids. At the height of the decree's enforcement, many cafés experienced weekly—and in some cases even daily—police inspections. In many cities, municipal governments attempted to shut down immigrant-owned Internet cafés under the auspices of "terrorism," though in most cases they were actually closed for neglecting to collect customers' identification data. In just two days of August 2005 alone, police sweeps were carried out across Italy against 7,318 call centers, Internet cafés, money transfer points, and halal butchers—spaces targeted as meeting points in Muslim communities (Camera dei Deputati 2005). A total of 32,703 people were identified, 341 were arrested, and 426 were charged with various crimes (Camera dei Deputati 2005). In addition, 701 expulsion procedures were initiated and 325 fines were levied against call centers, Internet cafés, and money transfers for "administrative irregularities" (Camera dei Deputati 2005). While butcher shops represent material incursions of cultural difference into the boundaries of Italian territory, Internet cafés and related businesses signal the formation and elaboration of communication and financial linkages with potentially dangerous elements *outside* of the Italian territory. Both types of establishments threaten Italian national security, but in markedly different ways.

While the Italian police used Internet cafés as a way to target "undesirable," "dangerous," or "marginal" populations (i.e., undocumented immigrants of color and Muslims), there was more to the focus on Internet cafés than simply efficient policing. As seen in the parliamentary discussions of the Pisanu Decree described earlier, Internet cafés also became shorthand for the sorts of dangerous transnational networking that are facilitated by the technology of the Internet. In other words, the Italian government's targeting of Internet cafés represented an effort to simultaneously fix mobile immigrant populations *and* the unruly networks of the Internet. Muslim immigrants were conflated with the "dark side" of the Internet, and this racial categorization took material form in the space of the Internet café. The Internet, after all, is both spatial *and* material, and this is perhaps most obvious in the Internet café. Individuals must negotiate the particularities of place—urban geographies, zoning laws, material infrastructure—that coalesce in the Internet café in order to gain access to the transnational flows of the Internet. The Internet café can therefore be understood as a material node in the unruly, spatially extended Internet, and because of its stability, its fixedness in place, it became a natural target for immigration control and antiterrorism policing efforts seeking to contain radical transnational communication and intervene in dangerous networks.

Circulation, Control, and Racialized Networks

In post-2005 Italy, an overarching sociotechnical imaginary of the Internet as a space of freedom was simultaneously linked to techno-utopian visions of innovation *and* to alarmist fears of terrorist networking that cannot be contained by the borders of the nation-state. For this reason, debates about the Pisanu Decree encompassed concerns about both the restriction of entrepreneurship and invasions of user privacy (i.e., the maintenance of an open and free Internet) and the need to control suspicious immigrants (i.e., the dangers of unrestricted online communication)—what Foucault ([2004] 2007, 18) described in his "Security, Territory, Population" lectures as the division between good and bad circulation. The official imaginary of the Internet in Italy as both *constructive* circulation and *dangerous* circulation is therefore deeply racialized, with the latter deployed against people of color, and Muslims in particular. This tension between freedom and control (Chun 2006) can also be read as an extension of an opposition that has been central to the structure of the Internet since its development—namely, what Galloway (2004, 8) describes as the contradiction between anarchic distribution, represented by the TCP/IP protocols, and rigidly controlled hierarchies, represented by the DNS protocol.

If the idea of race is central to the formation of the modern European nation-state (Gilroy 1987; Balibar 1991; Goldberg 2002; Foucault [1997] 2003), then the border regimes of Fortress Europe and the technologies of digital and biometric surveillance they employ are also about race and the management of difference. Indeed, as Browne (2012, 2015) argues, modern practices of surveillance have their roots in the regulation of the movement of enslaved and colonized people. These bordering practices, while not limited to territorial borders, have material and violent consequences (Pugliese 2013a) even as they come to encompass increasingly mundane and quotidian activities such as frequenting an Internet café

or responding to emails from family members in distant countries. These technologies allow for the policing of racial difference within the national body, and also constitute new types of racial subjects that can be categorized as Others on the basis of their social associations and technology use, as opposed to just their phenotype or biological makeup.

Studies of biometric borders as a mechanism for regulating circulation often emphasize a visual logic—the scanning of faces to reveal the "foreign terrorist in the nation" (Chun 2009, 25). Pugliese (2013b, 571), for instance, argues that biopolitical technologies of extraterritorialization constitute "regimes of statist visuality." Following this logic, the visual, face-centered cultures of social networking on the Internet (González 2009) provide new opportunities for panoptic facial scanning. As critical race theorists argue, however, race and classification are about much more than the visual—even Fanon ([1952] 2008; see Browne 2009) acknowledged that epidermalization implicated not only the gaze, but also interlinked psychological, structural, and spatial processes in the production of racial subjects. Thus, it is possible to think about Internet surveillance without privileging scopic metaphors, but rather by considering vision as one among many techniques of perception (Crary 2001).

In Italy, for instance, many Internet café owners installed video cameras to monitor their computer stations after the passage of the Pisanu Decree; in addition, businesses were required to register comprehensive floor plans with local police and track exactly which computer terminals their customers used and for how long. This optic surveillance, however, was inoperable if separated from its relationship to other information such as photocopies of passports and logs of Internet browsing and communication data (collected both through software installed on individual Internet café computers and at the level of the ISP). Surveillance, therefore, is not simply a matter of making threatening subjects visible, but is instead about forming *new* subjects from the assembly of discrete data points such as one's web traffic histories, online communications, patterns of Internet café use, and movement through space. This sort of "dataveillance" (Clarke 1994; Levi and Wall 2004; Amoore and de Goede 2005) works by compiling and processing raw data as inputs (van Dijk 2014) that, via algorithmic logics, can produce certain bodies and networks as "risky" (Epstein 2008, 179). Algorithmic war, Amoore (2009, 49) argues, is powerful precisely because of this invisibility. It creates "association rules" between people, places, objects, and events, using the prosaic and the everyday to make preemptive security decisions in a Foucauldian continuation of war by other means.

Unlike biometric surveillance, which attempts to make bodies visible as faces or organic molecules, Internet surveillance is (perhaps counterintuitively) also bound up with questions of placefulness: location, mobility (understood as movement through physical and virtual spaces), and spatially situated social associations. In an age of ubiquitous cybersurveillance, therefore, it is not only faces that must be scanned in order to unveil racial threats hidden within the body of the nation. The surveillance of Internet browsing and other technological practices involve the scanning of spatially extended *networks* as well.

Within the context of this sort of networked surveillance, it is not merely what one *is* that discloses a person as a threatening "raced Other," it is also that person's activities, movements, occupation of particular spaces, relations, and technological habits. As Noble (2018) argues, algorithms are not neutral; they are thoroughly suffused with the prejudices of their makers and in turn help to reinforce

and reproduce structural racism and inequality. In the case of Italy, surveillance "metadata" are filtered through stereotypical understandings of Muslim culture as inherently illiberal and premodern in order to produce a new form of identifiable racial subject (see Puar 2007)—the male, Muslim immigrant Internet café patron who has been radicalized by jihadist websites and is now a potential terrorist lurking within Italy's borders. In this way, traces of movement through physical (Internet café terminal) and virtual (transnational Internet networking) spaces become the (t)races, or what Harrell (2013) calls "phantasms," for algorithmically assembling categorizable, raced subjects.

Of course, this is a process always replete with contradictions and slippages. Surveillance, algorithmic and otherwise, may have as its goal comprehensive predictive power, but in practice it generates "actual asymmetries and uncertainties" (Crampton and Miller 2017, 5). The Pisanu Decree, for instance, was a blunt-edged tool that sweepingly conflated Muslims with undocumented immigrants and potential terrorists, regardless of their origins; in addition, Pisanu also ensnared tourists (Hooper 2005), who would arguably constitute an example of "good" (orderly, nonthreatening) circulation in the eyes of the Italian state. This was not a problem of misidentification—as Hacking (2006, 23) argues, categories actively transform the people being classified in a recursive "looping effect." In the Italian state's efforts to fix a particular kind of threatening racial subject on the basis of recognizable technological characteristics, however, the communities under surveillance consistently exceeded or evaded categorization. Tactics as simple as presenting false identification documents could effectively disrupt the associational logics of the decree. In addition, the racial distinction between economically entrepreneurial Internet circulation and dangerous religious Internet circulation faltered on the figure of the (Muslim) immigrant Internet café owner, a contradiction that would ultimately lead to Pisanu's repeal.

Conclusion: Beyond the Pisanu Decree to New Terrains of Control

> *Digital connectedness does not come as a utopian alternative to histories of dislocation, rejection and expulsion. . . . Furthermore, the use of digital technologies has created new forms of surveillance, bordering and monitoring access to Europe. Fortress Europe becomes a highly virtualized concept, whose paradox is being poised on embracing a project of expansion and inclusion versus digital and physical re-walling and refencing.*
>
> **—Ponzanesi and Leurs (2016)**

In the last decade, the Internet has emerged as an important mechanism for the regulation and enforcement of borders in Fortress Europe. Indeed, the spatial potentialities of the Internet do not make nation-states obsolete but instead offer new terrains for control. As the case of the Pisanu Decree reveals, imaginaries of technology are intimately linked to race, and produce new kinds of racial subjectivities through technologically specific modes of profiling. While the surveillance of online communications (email, social networking sites, forums, etc.), web browsing, money transfers, and charitable donations has emerged as an important field of scholarly research, however, this new wave of Internet surveillance and control has for the most part not been integrated with broader conversations about race on the Internet, nor has it been connected to discussions about transnational flows,

immigration, and border control. These lacunae are problematic because, as the case of Italy demonstrates, antiterrorism programs targeting the Internet are closely articulated with immigration control, border securitization, and racial profiling.

By neglecting to situate Internet surveillance and regulation within the context of broader debates about race and immigration, scholars risk overlooking the disproportionate impact of state-sanctioned Internet surveillance on marginalized communities of color. An unintended consequence of Edward Snowden's 2013 leaks of classified NSA documents has been a "whitewashing" of cybersurveillance—as Mohamad Tabbaa (2013) sardonically quipped in an editorial for *Salon*, "Suddenly, white people care about privacy incursions." Telecommunication surveillance and nonconsensual privacy incursions are indeed frighteningly pervasive in the contemporary moment; however, racializing digital surveillance has been a relatively unacknowledged yet profoundly troubling reality for people of color—and Muslims in particular—since 9/11. Politically, an STS-based understanding of race as a sociotechnical system allows us to consider the implications of Internet surveillance for both the transformation of contemporary racial and nationalist ideologies, and for the development of viable antiracist and antixenophobic practices.

It is important to note, however, that the techniques of surveillance are dynamic and shifting. Arguably, the time of the Internet café is passing, and the Pisanu Decree represented a snapshot in time of a particular effort in Italy to secure the Internet and monitor the people who use it. A 2012 report found that 70% of immigrants in Italy use the Internet, and of these, 65% percent browse the web from their own homes (Micheli 2012). The increasing ubiquity and affordability of personal Internet-connected devices is slowly shifting technological practices away from Internet cafés. While Internet cafés are no longer isolated by the Italian state as strategic sites of intervention into dangerous online networks, however, questions of space and placefulness are still important to any analysis of racializing surveillance. Perhaps signaling this transition, a 2010 report about terrorism in Italy described a suspect as having turned the space of his personal *living room* into a "virtual madrassa" (Bjorkman 2010, 241) linked to jihadist web forums and online resources.

As of January 1, 2012, Article 7 of the Pisanu Decree is no longer in force, following a lengthy and labyrinthine repeal process (*Punto Informatico* 2010; *Apogeonline* 2011; Scialdone 2011; Zambardino 2011; *ASAT* 2013). The eventual repeal of regulations on Internet cafés and Wi-Fi hotspots was justified due to concerns about privacy, business growth, and the difficulty of establishing and accessing public wireless Internet networks in Italy—questions of racism and immigrants' rights were never part of the public debate about the law. Rather, objections to the Pisanu Decree associated the "liberalization" of Internet cafés and Wi-Fi with political freedom, business development, and technological advancement—in other words, the techno-utopian belief that the Internet inherently "wants to be free."

But while identity documents are no longer required at Italian Internet cafés, most public wireless networks still require a lengthy user registration process (Monti 2013). And despite the repeal of the Pisanu Decree, Internet cafés are still sometimes subject to police surveillance. Similarly, Internet surveillance and monitoring in Italy continue, including increased attention to sex trafficking and online ISIS recruitment and radicalization rings. In addition, prompted by the EU, local governments and nongovernmental organizations have increasingly em-

braced information and communication technologies for immigrant integration (Borkert et al. 2009; Boccagni and Pasquinelli 2010; European Commission Joint Research Centre 2012), emblematic of a broader shift in Italian discourse and policy-making concerning immigration toward the goal of "integration." Finally, these developments must also be situated within the context of the intensified patrolling of the Mediterranean for refugees arriving to Italy by sea, including the absorption of Italy's Mare Nostrum search-and-rescue program into the EU-Frontex border management operation Triton (European Council on Refugees and Exiles 2014). This array of new border management and surveillance strategies targeting refugees and migrants—intervening in transnational digital communication networks and transnational maritime travel routes (Stierl 2015), as well as overland paths to and within Europe—represents diverse efforts to control circulation through the telescoping of borders both within and beyond the boundaries of the nation-state.

Notes

1. Following Browne (2012, 72), "racializing surveillance" refers to "moments when enactments of surveillance reify boundaries and borders along racial lines, and where the outcome is often discriminatory treatment."
2. See Ilten and McInerney (this volume) for a discussion about the significance of studying the social construction of ICTs and new media, rather than approaching these technologies simply as "tools."
3. While the Pisanu Decree covered many areas, I focus on Internet cafés in this chapter because they were significant objects of state concern during the law's implementation, as seen in legislative hearings and policing records.
4. A clause in a 2003 Italian bill that would have required ISPs to monitor Internet activity and retain data (including email data) for five years, which could then be turned over to the courts, was removed after fierce opposition by cyber-freedom activists, opposition parties, and the Italian Office for the Protection of Personal Data (Reporters without Borders 2004).
5. All translations by the author.

Works Cited

Adas, Michael. 1990. *Machines as the Measure of Man: Science, Technology, and Ideologies of Western Dominance*. Ithaca, NY: Cornell University Press.

Amoore, Louisa. 2009. "Algorithmic War: Everyday Geographies of the War on Terror." *Antipode* 41 (1): 49–69.

Amoore, Louisa, and Marieke de Goede. 2005. "Governance, Risk and Dataveillance in the War on Terror." *Crime, Law and Social Change* 34:149–73.

Ananthaswamy, Anil. 2011. "Welcome to the Age of the Splinternet." *New Scientist* 211 (2821): 42–45.

Angel-Ajani, Asale. 2000. "Italy's Racial Cauldron: Immigration, Criminalization, and the Cultural Politics of Race." *Cultural Dynamics* 12 (3): 331–52.

Apogeonline. 2011. "A Che Punto Sono le 'Leggi' di Internet?" January 10. www.apogeonline.com/filirossi/leggi-internet.

ASAT. 2013. "Internet e WiFi—Decreto Del Fare." July 24. www.asat.it/internet-e-wifi---decreto-del-fare/53-4558/.

Balibar, Etienne. 1991. "Is There a 'Neo-Racism'?" In *Race, Nation, and Class: Ambiguous Identities*, edited by Etienne Balibar and Immanuel Wallerstein, 17–28. London: Verso.

BBC. 2005a. "Italy Approves Anti-terror Steps." July 29. http://news.bbc.co.uk/2/hi/europe/4728873.stm.

———. 2005b. "Bombings Suspect Charged in Italy." August 1. http://news.bbc.co.uk/2/hi/4733867.stm.

Benjamin, Ruha. 2016. "Catching Our Breath: Critical Race STS and the Carceral Imagination." *Engaging Science, Technology, and Society* 2:145–56.

Bjorkman, Carl. 2010. "Salafi-Jihadi Terrorism in Italy." In *Understanding Violent Radicalisation: Terrorist and Jihadi Movements in Europe*, edited by Magnus Ranstorm, 231–55. New York: Routledge.

Boccagni, Paolo, and Sergio Pasquinelli. 2010. "The Potential of ICT in Supporting Immigrants in Domiciliary Care in Italy." Luxembourg: European Union Joint Research Centre, Institute for Prospective Technological Studies.

Boellstorff, Tom, Bonnie Nardie, Cecilia Pearce, and T. L. Taylor. 2012. *Ethnography and Virtual Worlds: A Handbook of Method*. Princeton, NJ: Princeton University Press.

Borkert, Maren, Pietro Cingolani, and Viviana Premazzi. 2009. "The State of the Art of Research in the EU on the Uptake and Use of ICT by Immigrants and Ethnic Minorities." 23991 EN. Seville, Spain: European Commission Joint Research Centre, Institute for Prospective Technological Studies. http://ipts.jrc.ec.europa.eu/publications/pub.cfm?id=2560.

Browne, Simone. 2009. "Digital Epidermalization: Race, Identity, and Biometrics." *Critical Sociology* 36 (1): 131–50.

——. 2012. "Race and Surveillance." In *Routledge Handbook of Surveillance Studies*, edited by Kirstie Ball, Kevin Haggerty, and David Lyon, 72–79. New York: Routledge.

——. 2015. *Dark Matters: On the Surveillance of Blackness.* Durham, NC: Duke University Press.

Burrell, Jenna. 2012. *Invisible Users: Youth in the Internet Cafés of Urban Ghana*. Cambridge, MA: MIT Press.

Camera dei Deputati. 2005. "Misure per prevenire il radicamento del fondamentalismo islamico sul territorio italiano - n. 2-01633." Seduta n. 676 del 22/9/2005. Dibatti svolti alla Camera nella XIV Legislatura. http://legislature.camera.it/_dati/leg14/lavori/stenografici/framevar.asp?sedpag=Sed676/s050.htm|STitolo9%2016.

Carter, Donald Martin. 2013. "Blackness over Europe: Meditations on Cultural Belonging." In *Africa in Europe: Studies in Transnational Practice in the Long Twentieth Century,* edited by Robbie Aitken and Eve Rosenhaft, 201–13. Liverpool: University of Liverpool Press.

Castells, Manuel. 2000. *The Rise of the Network Society*. 2nd ed. Malden, MA: Blackwell.

Celeste, Sofia. 2005. "Want to Check Your E-mail in Italy? Bring Your Passport." *Christian Science Monitor*, October 4. www.csmonitor.com/2005/1004/p07s01-woeu.html.

Chun, Wendy Hui Kyong. 2006. *Control and Freedom: Power and Paranoia in the Age of Fiber Optics*. Cambridge, MA: MIT Press.

——. 2009. "Introduction: Race and/as Technology; or, How to Do Things to Race." *Camera Obscura* 24 (1): 7–35.

——. 2010. "Imaged Networks: Digital Media, Race, and the University." In *Universities in Translation the Mental Labor of Globalization*, edited by Brett de Bary, 341–54. Hong Kong: Hong Kong University Press.

Clarke, Roger. 1994. "Dataveillance: Delivering 1984." In *Framing Technology: Society, Choice, and Change*, edited by Leila Green and Roger Guinery, 117–30. London: Routledge.

Cole, Jeffrey. 1997. *The New Racism in Europe: A Sicilian Ethnography*. Cambridge: Cambridge University Press.

Coleman, Beth. 2009. "Race as Technology." *Camera Obscura* 24 (1): 176–206.

Conversione in Legge, con Modificazioni, del Decreto-Legge 27 Luglio 2005, n. 144, Recante Misure Urgenti per il Contrasto del Terrorismo Internazionale. 2005. Legge 31 Luglio 2005, n. 155. Accessed January 6, 2015. www.camera.it/parlam/leggi/05155l.htm.

Crampton, Jeremy, and Andrea Miller. 2017. "Introduction: Intervention Symposium—'Algorithmic Governance.'" *Antipode*, May 19. https://antipodefoundation.org/2017/05/19/algorithmic-governance/.

Crary, Jonathan. 2001. *Suspensions of Perception: Attention, Spectacle, and Modern Culture*. Cambridge, MA: MIT Press.

Daniels, Jessie. 2009. *Cyber Racism: White Supremacy Online and the New Attack on Civil Rights*. Lanham, MD: Rowman & Littlefield.

Decreto-legge 144/05: Misure Urgenti Per il Contrasto del Terrorismo Internazionale. C. 6045 Governo, Approvato dal Senato C. 6045 Governo (Esame e Conclusione). 2005. Seduta di Venerdi 29 Luglio 2005. Dibatti Svolti alla Camera nella XIV Legislatura. http://legxiv.camera.it/_dati/leg14/lavori/bollet/200507/0729/HTML/frontesp.htm.

Dery, Mark. 1994. *Flame Wars: The Discourse of Cyberculture*. Albany: State University of New York Press.

Disegno di Legge di Conversione, con Modificazioni, del Decreto-Legge n. 144 del 2005: Misure Urgenti per il Contrasto del Terrorismo Internazionale (Approvato dal Senato) (A.C. 6045) (Discussione ed approvazione). 2005. Seduta n. 666 di Sabato 30 Luglio 2005. Dibatti Svolti alla Camera nella XIV Legislatura. http://legxiv.camera.it/_dati/leg14/lavori/stenografici/sed666/s000r.htm.

Drayton, Richard. 2000. *Nature's Government: Science, Imperial Britain, and the "Improvement" of the World.* New Haven, CT: Yale University Press.

Epstein, Charlotte. 2008. "Embodying Risk. Using Biometrics to Protect the Borders." In *Risk and the War on Terror*, edited by Louise Amoore and Marieke De Goede, 178–93. New York: Routledge.

European Commission Joint Research Centre. 2012. "ICT for Integration of Immigrants & Ethnic Minorities (IEM)." Brussels, Belgium: European Commission Joint Research Centre, Information Society Unit. http://is.jrc.ec.europa.eu/pages/EAP/eInclusion/IEM.html.

European Council on Refugees and Exiles. 2014. "Mare Nostrum to End—New Frontex Operation Will Not Ensure Rescue of Migrants in International Waters." October 10. http://ecre.org/component/content/article/70-weekly-bulletin-articles/855-operation-mare-nostrum-to-end-frontex-triton-operation-will-not-ensure-rescue-at-sea-of-migrants-in-international-waters.html.

European Parliament and Council. 2002. "Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (Directive on Privacy and Electronic Communications)." http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:EN:HTML.

Everett, Anna. 2009. *Digital Diaspora: A Race for Cyberspace*. New York: State University of New York Press.

Fanon, Frantz. [1952] 2008. *Black Skin, White Masks*. New York: Grove Press.

Forlano, Laura, and Kat Jungnickel. 2015. "Hacking Binaries/Hacking Hybrids: Understanding the Black/White Binary as a Socio-technical Practices." *Ada* 6. http://adanewmedia.org/2015/01/issue6-forlano-jungnickel/.

Foucault, Michel. [1997] 2003.*"Society Must Be Defended: Lectures at the Collège de France, 1975–1976*. Edited by Mauro Bertani and Alessandro Fontana. Translated by David Macey. New York: Picador.

———. [2004] 2007. *Security, Territory, Population: Lectures at the Collège de France, 1977–1978.* Edited by Michel Senellart. Translated by Graham Burchell. New York: Picador.

Galloway, Alexander R. 2004. *Protocol: How Control Exists after Decentralization*. Cambridge, MA: MIT Press.

Gilroy, Paul. 1987. *There Ain't No Black in the Union Jack: The Cultural Politics of Race and Nation*. Chicago: University of Chicago Press.

Goldberg, David Theo. 2002. *The Racial State*. Oxford: Wiley-Blackwell.

González, Jennifer. 2009. "The Face and the Public: Race, Secrecy, and Digital Art Practice." *Camera Obscura* 24 (1): 37–65.

Goody, Jack. [1971] 1980. *Technology, Tradition, and the State in Africa*. Cambridge: Cambridge University Press.

Hacking, Ian. 2006. "Making Up People." *New York Review of Books* 28 (16): 23–26.

Haraway, Donna. 1989. *Primate Visions: Gender, Race, and Nature in the World of Modern Science*. New York: Routledge.

———. 1991. *Simians, Cyborgs and Women: The Reinvention of Nature*. New York: Routledge.

Harrell, D. Fox. 2013. *Phantasmal Media: An Approach to Imagination, Computation, and Expression*. Cambridge, MA: MIT Press.

Hooper, John. 2005. "Passport to Surf." *Guardian*, September 29. www.theguardian.com/news/blog/2005/sep/29/passporttosur.

Informativa del Governo Concernente la Prima Applicazione della Recente Normativa sul Contrasto del Terrorismo Internazionale. 2005. Seduta n. 716 di Venerdi 2 Dicembre 2005. Dibatti Svolti alla Camera nella XIV Legislatura. http://legxiv.camera.it/_dati/leg14/lavori/stenografici/sed716/s000r.htm.

Jasanoff, Sheila, and Sang-Hyun Kim. 2009. "Containing the Atom: Sociotechnical Imaginaries and Nuclear Power in the United States and South Korea." *Minerva* 47 (2): 119–46.

Kington, Tom. 2009. "Anti-immigrant Italians Find a New Foe: Food from Abroad." *Guardian,* November 15. www.theguardian.com/world/2009/nov/15/italys-kebab-war-hots-up.

Kraemer, Jordan. 2013. "Friend or *Freund*: Social Media and Transnational Connections in Berlin." *Human-Computer Interaction* 29 (1): 53–77.

Landzelius, Kyra, ed. 2006. *Native on the Net: Indigenous and Diasporic Peoples in the Virtual Age*. New York: Routledge.

Levi, Michael, and David S. Wall. 2004. "Technologies, Security, and Privacy in the Post-9/11 European Information Society." *Journal of Law and Society* 31 (2): 194–220.

Licklider, J.C.R., and Robert Taylor. [1968] 1990. "The Computer as a Communication Device." Reprinted in *In Memoriam: J.C.R. Licklider 1915–1990*, Research Report 61, Digital Equipment Corporation Systems Research Center (August), 21-41. http://memex.org/licklider.pdf.

Magnet, Shoshana. 2011. *When Biometrics Fail: Gender, Race, and the Technology of Identity.* Durham, NC: Duke University Press.
Malcomson, Scott. 2016. *Splinternet: How Geopolitics and Commerce Are Fragmenting the World Wide Web.* New York: OR Books.
McGahan, Christopher L. 2008. *Racing Cyberculture: Minoritarian Art and Cultural Politics on the Internet*. New York: Routledge.
McLelland, Mark J. 2008. "'Race' on the Japanese Internet: Discussing Korea and Koreans on '2-Channeru.'" *New Media & Society* 10 (6): 811–29.
McLuhan, Marshall. [1962] 2011. *The Gutenberg Galaxy: The Making of Typographic Man*. Toronto: University of Toronto Press.
Mellino, Miguel. 2012. "De-provincializing Italy: Notes on Race, Racialization, and Italy's Coloniality." In *Postcolonial Italy: Challenging National Homogeneity*, edited by Cristina Lombardi-Diop and Caterina Romeo, 83–99. New York: Palgrave Macmillan.
Merrill, Heather. 2006. *An Alliance of Women: Immigration and the Politics of Race.* Minneapolis: University of Minnesota Press.
Micheli, Massimo. 2012. "Il 70% degli Immigrati Naviga Sul Web." *Italiani nel Mondo*, February 1. www.italianitalianinelmondo.com/2010/notizie.php?id=640&s=4.
Ministero della Giustizia. 2012. "La Radicalizzazione Del Terrorismo Islamico: Elementi Per Uno Studio Del Fenomeno Di Proselitismo in Carcere." Numero 9. Quaderni ISSP. Rome: Ministero della Giustizia, Dipartimento dell'Amministrazione Penitenziaria.
———. 2010. "Iniziative dell'Italia: Sicurezza, Immigrazione e Asilo." Rome: Ministero dell'Interno. www.cnel.it/application/xmanager/projects/cnel/attachments/shadow_documentazioni_attachment/file_allegatos/000/142/460/0843_Opuscolo_ITA.pdf.
Mitchell, Timothy. 2002. *Rule of Experts: Egypt, Techno-Politics, Modernity.* Berkeley: University of California Press.
Monti, Andrea. 2013. "Il Decreto Pisanu è morto, I suoi obblighi, no." *Ictlex*, April 30. www.ictlex.net/?p=1475.
Nakamura, Lisa. 2002. *Cybertypes: Race, Ethnicity, and Identity on the Internet*. New York: Routledge.
———. 2007. *Digitizing Race: Visual Cultures of the Internet*. Minneapolis: University of Minnesota Press.
Nelson, Alondra. 2002. "Introduction: Future Texts." *Social Text* 20 (2): 1–15.
Nguyen, Mimi. 2003. "Queer Cyborgs and New Mutants: Race, Sexuality, and Prosthetic Sociality in Digital Space." In *AsianAmerica.net: Ethnicity, Nationalism, and Cyberspace*, edited by Rachel Lee and Sau-Ling Wong, 281–305. New York: Routledge.
Noble, Safiya Umoja. 2018. *Algorithms of Oppression: How Search Engines Reinforce Racism*. New York: New York University Press.
Omi, Michael, and Howard Winant. 1986. *Racial Formation in the United States: From the 1960s to the 1980s*. New York: Routledge.
OpenNet Initiative. 2010. "Italy." December 15. https://opennet.net/research/profiles/italy
Pavis, Theta. 2000. "Euros Catching up with Net." *Wired*, April 7. www.wired.com/2000/04/euros-catching-up-with-net/?currentPage=1.
Pearce, Katy E., and Sarah Kendzior. 2012. "Networked Authoritarianism and Social Media in Azerbaijan." *Journal of Communication* 62 (2): 283–98.
Phillip, Kavita. 2003. *Civilizing Natures: Race, Resources, and Modernity in Colonial South India*. New Brunswick, NJ: Rutgers University Press.
Ponzanesi, Sandra, and Koen Leurs. 2016. "On Digital Crossings in Europe." *Crossings* 5 (1): 3–22.
Prakash, Gayan. 1999. *Another Reason: Science and the Imagination of Modern India*. Princeton, NJ: Princeton University Press.
Provincia Di Reggio Emilia. 2006. "Terrorismo Islamico, a Reggio Servono Più Controlli." September 1. www.provincia.re.it/page.asp?IDCategoria=703&IDSezione=5244&ID=93292.
Puar, Jasbir. 2007. *Terrorist Assemblage: Homonationalism in Queer Times.* Durham, NC: Duke University Press.
Pugliese, Joseph. 2013a. *State Violence and the Execution of Law: Biopolitical Caesurae of Torture, Black Sites, and Drones.* New York: Routledge.
———. 2013b. "Technologies of Extraterritorialization, Statist Visuality, and Irregular Migrants and Refugees." *Griffith Law Review* 22 (3): 571–97.
Punto Informatico. 2010. "Decreto Pisanu, Pronto il Cestino?" October 6. http://punto-informatico.it/3004602/PI/News/decreto-pisanu-pronto-cestino.aspx.

Reporters without Borders. 2004. "Internet under Surveillance 2004—Italy." www.refworld.org/docid/46e6918b21.html.

Rheingold, Howard. 1993. *The Virtual Community: Homesteading on the Electronic Frontier*. New York: Addison-Wesley.

Said, Edward. [1978] 2014. *Orientalism*. New York: Vintage.

Sandoval, Chela. 2000. *Methodology of the Oppressed*. Minneapolis: University of Minnesota Press.

Sanminiatelli, Maria. 2005. "Anti-terror Law Forces Cybercafé Owners to Take Names." *USA Today*, December 8. http://usatoday30.usatoday.com/tech/news/computersecurity/2005-12-08-cybercafe-law_x.htm.

Scialdone, Mario. 2011. "Decreto Pisanu, l'Addio Definitivo?" *In tutta sincerità . . .* , December 30. http://scialdone.blogspot.com/search/label/decreto%20milleproroghe.

Shklovski, Irina, Janet Vertesi, and Silvia Lindtner. 2013. "Introduction to This Special Issue on Transnational HCI." *Human-Computer Interaction* 29 (1): 1–21.

Stierl, Maurice. 2015. "The WatchTheMed Alarm Phone. A Disobedient Border-Intervention." *Movements* 1 (2). http://movements-journal.org/issues/02.kaempfe/13.stierl--watchthemed-alarmphone.html.

Stoler, Ann Laura. [2002] 2010. *Carnal Knowledge and Imperial Power: Race and the Intimate in Colonial Rule*. Berkeley: University of California Press.

Tabbaa, Mohamad. 2013. "Suddenly, White People Care about Privacy Incursions." *Salon*, June 13. www.salon.com/2013/06/13/suddenly_white_people_care_about_privacy_incursions/.

Terrorismo Ed Eversione. 2004. "Relazione Al Parlamento—Anno 2004." Rome: Ministero dell'Interno.

Thompson, Derek. 2010. "The Fall of the Internet and the Rise of the 'Splinternet.'" *Atlantic*, March 8. www.theatlantic.com/business/archive/2010/03/the-fall-of-the-internet-and-the-rise-of-the-splinternet/37181/.

Tsing, Anna L. 2005. *Friction: An Ethnography of Global Connection*. Princeton, NJ: Princeton University Press.

Turner, Fred. 2006. *From Counterculture to Cyberculture: Stewart Brand, the Whole Earth Network, and the Rise of Digital Utopianism*. Chicago: University of Chicago Press.

van Dijk, José. 2014. "Datafication, Dataism and Dataveillance: Big Data between Scientific Paradigm and Ideology." *Surveillance & Society* 12 (2): 197–208.

Winner, Langdon, ed. 1989. *The Whale and the Reactor: A Search for Limits in an Age of High Technology*. Chicago: University of Chicago Press.

Yalla Italia. 2012. "Sempre Più Italiani Lavorano per gli Immigrati." April 26. www.yallaitalia.it/2012/04/sempre-piu-italiani-lavorano-per-gli-immigrati/.

Zambardino, Vittorio. 2011. "Ve lo Ricordate il Decreto Pisanu? Solo Adesso, Forse, Se Ne Va Davvero." *La Reppublica*, December 31. http://archive.is/G3AWU.