CHAPTER 6

Grasping Surveillance

It's not easy to believe in the government. But we have to believe in something. We need to come together to make the government better, to trust it more. I have to take on my responsibility independent of whether I believe in the government or not. We have to meet our responsibility. So, I see this program independently of whether the authorities do what they're supposed to. We as citizens should fulfill our obligation. At the end of the day, we have to think of the future, in our welfare, independent of the difficulties. And that means acting with values, involving ourselves in social activities and programs. Without participation, it would be worse for everyone.

—Zacatecas resident registering with the REPUVE

6.1 THE MORE THINGS CHANGE . . .

Having left office at the end of 2012, Felipe Calderón and his crusade against insecurity have passed from the public stage in Mexico. But the problem of insecurity has not. During his campaign and first years in office, Enrique Peña Nieto sought to shift the public's attention away from security issues and toward economic and social policy. The hallmark of this effort was the Pact for Mexico, an accord signed by the president and leaders of the three major political parties to put aside political differences and move the country forward through cooperation in five key areas. These included agreements for (1) "a society of rights and liberties," which "achieves the inclusion of all social sectors and reduces the high levels of inequality that exist today between the people and regions of our country"; (2) "economic growth, employment, and competitiveness," whereby the "state should generate the conditions that permit for economic growth that results in the creation of stable and well-paying jobs"; (3) "security and justice," whose "principal objective . . . will be the recovery of peace and liberty to diminish violence"; (4) "transparency, accountability, and combatting corruption," which recognizes that "transparency and accountability are two tools of democratic states to elevate the confidence of citizens in their government"; and (5) "democratic governability," in which "the political plurality of the country is a undeniable reality derived from a long and incomplete process of democratic transition."[1]

While the pact was criticized as an antidemocratic measure bypassing the authority of the Congress,[2] it did help set a different tone for the new government. And the Peña Nieto administration built upon the pact by passing education reform aimed at increasing assessment of student learning and teacher training; telecommunications reform seeking to break media monopolies; and energy reforms designed to modernize the oil sector by privatizing Mexican Petroleums (PEMEX), the state-owned oil company that is a symbol of national identity dating back to Lázaro Cárdenas's nationalization of the country's oil reserves in 1938.[3]

Reality, however, has not followed the president's script. According to federal crime statistics, homicides have supposedly decreased since Peña Nieto took office. But independent reporting has found the rate consistent with the Calderón era, with over fifty-seven thousand deaths recorded in the first twenty months of the Peña Nieto administration.[4] And if the Pact for Mexico succeeded in capturing the public's attention during this time, the disappearance of forty-three students from the Raúl Isidro Burgos Rural Teachers' College of Ayotzinapa in September 2014 dramatically disrupted the federal government's efforts to manage the public's perception of insecurity. The kidnapping and presumed assassination of the young men who had dedicated themselves to careers in teaching, carried out by the local mayor in conjunction with police forces and a local crime syndicate, rekindled the wrath of a public fed up with the state's complicity in crime. The crimes, together with the inability of state authorities to locate the students' bodies, fueled demonstrations across the country under the banner of "Fue el Estado!" (It was the State!). In response, Peña Nieto did what Felipe Calderón and Vicente Fox had done before him: he announced the creation of a new federal police force—the National Gendarmerie—styled after France's and Chile's militarized national police forces, which would regain territory lost to organized crime through the increased use of cutting-edge technology and intelligence gathering.[5]

Outside Mexico, meanwhile, adoption of surveillance technologies to combat insecurity continues apace. Regionally, the problems of violence and organized crime plaguing Mexico exist in other Latin American countries, and national governments have turned to anonymized mobile device reporting, vehicle control systems, integrated telecommunications networks, video surveillance cameras, and the like in response.[6] In the United States, the killing of innocent people by drone strikes in the Middle East, ongoing revelations about the National Security Agency's massive domestic and international spying operations, and the use of excessive force by local police forces have drawn criticism. This criticism has prompted the federal government to define the use of drones for targeted killings,[7] limit domestic data collection,[8] and reduce the transfer of used military equipment to domestic police forces.[9] But reliance on surveillance technologies against insecurity remains. Globally, national governments use surveillance technologies in many of the same applications described in this book, and authoritarian regimes buy wares from US, Canadian, and European companies to monitor and punish dissenters who are defined as security threats.[10]

With these trends as a backdrop, what lessons does this examination of the Calderón administration's RENAUT, CEDI, and REPUVE programs hold? This concluding chapter attempts to answer this question by reviewing four thematic binaries central to understanding surveillance technologies and the state: visibility/tactility, strength/weakness, determinism/emergence, and fatalism/engagement. These ideas, taken together, underscore that while surveillance technologies might envision a future of tighter governmental control through grabbing hold of the materiality of society, the structure of society that has taken shape over the course of modernity ensures that a space for political action remains, which opens up opportunities for the citizenry to shape the fate of surveillance technologies and governance in the future.

6.2 VISIBILITY AND TACTILITY

Thinking on surveillance tends to privilege sight as a human sense. This is understandable. A fairly recent term dating back to the French Revolution's Reign of Terror, when surveillance committees were formed to monitor suspicious people and political dissidents, "surveillance" derives from the French prefix *sur* (over) and root *veiller* (to watch) and means "to watch over."[11] It was in this sense that Michel Foucault used the word in *Discipline and Punish* (whose French title is

Surveiller et punir), the seminal work that helped popularize the term in the academy.

The emphasis on visibility and sight has endured in our imaginations. Recent scholarship in surveillance studies has shifted this understanding, however, by describing how information technologies such as radio-frequency identification (RFID) tags, biometric cards, mobile devices, personal computers, and the networks that link these devices have transformed surveillance into "dataveillance."[12] The histories of the mobile telephone registry, personal identity card, and automobile registry in Mexico provide detailed case studies of the technical and administrative procedures required to collect data on communications, personal identity, and mobility. And what these cases show is that surveillance technologies operate not only through *visibility* and *watching over people,* but also through *tactility* and *taking hold of and remaining in touch with the materiality of both people and things.* Creating a national identity card based on biometric data requires that the human body be probed and contacted in different ways. Fingers need to be touched and recorded. Irises need to be scanned. These data are then encoded into bar codes and other formats that are stored both in the card and the digital databases of the government. Those databases of the state must then be integrated to eliminate redundancies. Creating a national automobile registry requires that the body of the car be examined, inspected, and touched in order to record three instances of a vehicle identification number inscribed on it. That information is then scanned into government databases and inscribed into RFID tags that are applied directly to vehicles' windshields. The public and private databases related to automobility are then merged to ensure "legal certainty."

This emphasis on touch and adhesion is why it is meaningful to speak of *prohesion* rather than surveillance. If surveillance is understood as "watching over people" for the sake of affecting their behavior, the histories of surveillance technologies in Mexico reveal an operation in which authorities use technological means to manipulate the stickiness or viscosity of the things that energize social life so as to better order society. With these technologies, authorities in Mexico continue an effort dating back to the founding of the nation to manage the materiality of communications, identification, and mobility.

The distinction between visibility and tactility is important for understanding the logic of governmental power today. For the state authorities of the eighteenth and nineteenth centuries studied by Foucault, surveillance and the constant monitoring of people allowed behaviors to be observed, comparisons between individuals to be made, ranks to be assigned, and knowledge to be generated that formed the basis of diverse disciplines or fields of social-scientific expertise. "In short," Foucault noted on surveillance, "it normalizes."[13] Through this operation, surveillance provided the basis for *discipline,* for ordering the chaotic masses of the natural and social worlds into individualized subjects and units. For federal authorities in Mexico who sought to realize the National Registry of Mobile Telephone Users (RENAUT), Citizen Identity Card (CEDI), and Public Registry of Vehicles (REPUVE), *prohesion* enabled registers of the objects and subjects circulating in society to be generated, evidence of their existence to be recorded, a connection to their materiality to be established, and comparisons between those things and officials records to be made. This is not a power interested in individualizing and normalizing the masses, as those individuations have already been made. It is rather a power seeking to match those objects and subjects that circulate in society with the data that exists about them and to localize them or ascertain their presence at a particular time and place. Prohesion, then, allows for the authentication of both people and things. And by this operation, prohesion provides the basis for *security,* for holding onto or preserving the order of subjects and objects in the world as it is.

The distinction between discipline and security has been drawn before, if not in these terms. Foucault already in 1978 described security as a third form of power distinct from sovereign and disciplinary power.[a] What Foucault termed security can be equated to what Gilles Deleuze referred to as "societies of control," where "we no longer find ourselves dealing with the mass/individual pair" present in the disciplinary society—"individuals have become 'dividuals,' and masses, samples, data, markets, or 'banks.'"[14] The dataveillance technologies of the control society are used to "social sort"[15] individuals in countless

[a] "Baldly," Foucault writes, "we could say that sovereignty is exercised within the borders of a territory, discipline is exercised on the bodies of individuals, and security is exercised over a whole population," where population "will be considered as a set of processes to be managed at the level and on the basis of what is natural in these processes." Put more plainly, security for Foucault is liberal governance, where the state intervenes in social relations so as to create "natural" relations that will provide the conditions for the organic growth of the economy, health, and so forth (Foucault, *Security, Territory, Population,* 11).

social settings: safe/legitimate and dangerous/illegitimate travelers at borders,[16] desirable and undesirable citizens on the streets,[17] automobility and pedestrian mobility at urban intersections,[18] good risks and bad risks for criminal rehabilitation in courts and prisons,[19] and so on. In Mexico, the phone registry, personal identity card, and automobile registry were launched with security as the explicit goal. Authorities wanted to sort between legitimate phones and stolen devices, suspicious and reputable individuals, and dubious and trustworthy motor vehicles.

But if this has been said before, examination of the Mexican government's attempts to implement prohesive technologies raises additional points. Significantly, discipline and security exhibit different concerns on the part of authorities relative to the worlds they look to govern. Discipline entails a missionary logic of transforming and ordering an external world thought to be defined by chaos, disorder, and danger. In the face of the plague, the healthy individual can be created. Out of the unimpressive military recruit, the efficient soldier can be crafted. From the untrained child, the educated student can be molded. From the common criminal, the reformed citizen can be made. Through the artful application of disciplinary techniques—enclosure, partitioning, functional sites, ranks, examinations, time tables—whatever mass of social or natural material can be broken down and remade into individual, productive units. Security, in contrast, carries a custodial logic of preserving that order or advantage that has been won over the world. In the face of terrorist or criminal risk that would disrupt the social order, the terrorist can be sorted out to preserve the status quo. In the face of environmental risk that would threaten the natural conditions necessary to maintain the population, the pollutant can be identified and neutralized to protect the natural order. In the face of disease risks, the infected person can be isolated to maintain the health of the population as a whole. Through the artful application of security techniques—the recording of identities, the tagging of bodies, the monitoring of information, the analysis of statistics—whatever collection of ordered elements can be preserved from risks and threats.

A conservativism is present with security, a fear or anxiety of loss, that is absent with discipline. Discipline is oriented outward and toward the future; it sets out into the world to colonize and conquer. Security is oriented inward and toward the present;[20] it sets up apparatuses to keep the world as it is. In contemporary society, a culture of insecurity reigns, which produces "the insecurity subject" who "is afraid but can effectively sublimate these fears by engaging in preparedness activities."[21]

In Mexico, the context of insecurity breeds a fear that automobiles can easily be stolen, that mobile telephones can be taken and used to extort money, and that family members can be kidnapped. Security measures are intended to provide the confidence that individuals will be able to maintain their hold on these valued items and their place in this valued social order.

More importantly, the distinction between surveillance and prohesion illustrates how discipline and security differ with relation to subjects. At its core, discipline involves subjectification—creating enclosures, partitioning people, and erecting functional sites where constant surveillance provides the means for shaping the human soul and creating the subject. Mexican authorities in the early twentieth century pursued roadway safety by responsibilizing motorists, by requiring them to pass driving tests, mark registration numbers on their vehicles, and carry infraction booklets to enable monitoring by police officers. But security is largely indifferent to human subjectivity. At its core, security involves conservation—creating inventories of things, tagging each one, and keeping them monitored through prohesion to protect the social order that modernity has brought forth. Mexican authorities today pursue automotive security by certifying motor vehicles, inspecting their vehicle identification numbers, and tagging them with RFID chips to automate monitoring by electronic scanners.

In contrast to discipline and surveillance, security through prohesion casts its focus beyond the human subject and its soul to the materiality of things that underlie collective agency in society. To stop the terrorist or criminal, security through prohesion would disable the automobiles, phones, and weapons that enable wrongdoing. Such a strategy matches what has been termed "targeted governance,"[22] where problems such as alcoholism are managed through drug interventions that target specific aspects of the person's biological being rather than more holistic (and complicated) interventions that seek to discipline the self. Prohesion combats crime through the targeted governance of telephones and cars rather than more holistic interventions against the norms and conduct of persons.

A certain distrust of the human subject is detected here—individuals cannot be trusted to preserve the social order themselves. As Benjamin Goold has noted, "The increased use of surveillance technologies might send a particularly negative message to members of the public about how the state views them and the extent to which they can expect the state to trust them."[23] If everyone is a suspect, the simplest way to secure society is to connect the circuits of control directly to the materiality of collective agency.

As the case studies of monitoring programs in Mexico demonstrate, this distrust extends to the state itself. In addition to adhering sentinels to the materiality of collective agencies, prohesion also attempts to integrate the state agencies that have emerged over the course of modernity to govern society. State authorities in charge of telecommunications, tax rolls, automobile licenses and registrations, voter rolls, population rolls, and so forth are made to cohere to one another to improve the state's hold on collective agency. But whereas the "interoperability" and "integration" of monitoring systems[24] are often perceived as an indication of the potency of dataveillance, they here speak to the lack of trust in authorities by authorities.[25] In Mexico, this lack of trust is pronounced. State officials openly say that police officers and other state employees cannot be trusted to carry out the law and protect the social order.[26] The telephone registry, personal identity card, and vehicle registry are ways in which the governance of telecommunications, personal identity, and automobility can be streamlined to increase efficacy. In a sense, then, prohesion evidences a belief that humans, be they the governed or the governors, simply cannot be entrusted with that which security aims to preserve.

As Foucault noted on multiple occasions, the presence of security as a new mode of power does not signify the passing of discipline or sovereign power. They coexist. Nevertheless, the shift to security with prohesion as the means for carrying it out would have serious consequences. Operating by attaching to the substance of our daily lives, prohesion can be particularly invasive. Personal privacy is under assault in various ways under the new surveillance, as the details of our lives get collected by private companies specializing in data management, are traded between public and private entities, or are hacked by digital criminals. Security can also be unjust. The poorest and most vulnerable in society are surveilled the most.[27] As a consequence, the divisions between the haves and have-nots are reinforced, an outcome that aligns with the conservative logic of security to preserve the social order.

In addition to invasions of privacy and the deepening of social inequalities, prohesion reveals a further, more worrisome dimension of security. In its aversion to human subjectivity, prohesion threatens the individual subject. Discipline sought to mold human subjectivity through constant attention to the minute details of people's lives. It represented a culmination of sorts in a "great tradition of the eminence of detail, [in which] all the minutiae of Christian education, of scholastic or military pedagogy, all forms of 'training' found their place easily enough" in the disciplinary society.[28] Security, however, disregards the toilsome, costly, mundane work of keeping watch over people in favor of simply attaching to the materiality of society. As a result, the formation of the subject is no longer a priority. Others have noted an analogous dynamic in speaking of the "data doubles" and "doppelgangers"[29] that dataveillance creates and acts upon in place of physical, autonomous subjects.[30] As Charlotte Epstein has put it, "When the human body is no longer so clearly upheld as the recipient of rights, as the subject of politics, it is not so clear that it is anything more than just a living object, or indeed an animal-to-be-managed."[31] In security, people are reduced from political subjects to physical bodies to be administered.

Beyond this, basic elements of the liberal political order designed to promote subjectivity find themselves under assault in security. In attempting to secure the social order through materiality rather than subjectivity, prohesion alters the individual's grip on the world in subtle but fundamental ways. For one, choice is moderated by mandatory actions that are required in the security society. The REPUVE requires motorists in Mexico to enroll in the automobile registry and adhere RFID tags to their vehicles. The CEDI requires citizens in Mexico to possess personal identification cards. And the RENAUT requires mobile telephone users in Mexico to register their phone numbers with the government. The cost of not doing so is the risk of not being able to access key services central to daily life in contemporary society. Drivers who do not register their vehicles could be restricted from accessing roadways activated by RFID stickers. People without identification cards could be denied social services. And callers who do not register their phones could be threatened with cessation of their cellular service. In the same way, air travelers throughout the world have little choice but to comply with nebulous requirements to publicly disrobe at security checkpoints and even less power to remove their personal communications and data from governmental and private-sector databases.

Second, property rights are slowly chipped away as the state seeks to attach itself to the things of daily life. Drivers in Mexico are mandated to have state-issued RFID devices adhered to their windshields, with little choice as to where the admittedly unsightly sticker is placed. The stickers are present and registered with the state at the point of sale, they cannot be legally removed, and they must be replaced if the windshield is replaced. The windshield ceases to belong to vehicle owners in the way it once did. Consequently, while drivers have never possessed their vehicles entirely (the plate that legally identifies the car belongs to the state and laws commonly proscribe tinted windows and other modifications), the state's placement of RFID stickers colonizes a new portion of the automobile—the windshield—which further limits ownership. Similarly, mobile telephones that are not registered with the state or do not comply with protocol requirements are denied access and operability, thus requiring the purchase of a new device that is already connected to networks of control. Vehicles and telephones still belong to their rightful owners, but in attempting to secure these objects, users are required to surrender aspects of ownership to the state and programs that would protect them.

Third, self-determination is restricted by biometric identification. Electronic identity cards that identify individuals according to their biological material rather than their names result in a diminished space for individuals to define themselves before authorities. This can be seen as an extension of a long trend in Mexican history. Indigenous peoples of Mexico were forced to identify themselves within the naming practices and structure of Hispanic society. But under security, even that diminished capacity to name oneself is removed. With biometric information, one's biology "anchors" identity.[32]

Thus, security by prohesion—by diminishing choice, private property, and self-determination—threatens those fundamental elements of liberal society that ensure subjectivity. And the modern liberal subject is left at risk. Paradoxically, then, if the disciplinary society and visibility carried the goal of subjectifying society, then the tools being used to defend that social order, that subject, and the material things by which it defines itself serve to slowly extinguish the subject.[b]

[b] This concern resonates with arguments that critical theorists of a generation ago made concerning technology. The "Megamachine" of modern industrial society, cautioned Lewis Mumford, would eventually "reduce all forms of life and culture to those that can be translated into the current system of scientific abstractions, and transferred on a mass basis to machines and electronic apparatus" (Mumford, "Technics and the Nature of Man," 315). But an important distinction can be made. While the Megamachine and Technique (Ellul, "Technological Order") reduced the subject to one dimension (Marcuse, *One-Dimensional Man*), they still required a substantial investment of human action and oversight in order to cultivate that dimension. With security, the subject is bypassed altogether and the conditions under which she or he would develop, even along a single trajectory of technical specialization and market consumption, are restricted.

6.3 STRENGTH AND WEAKNESS

If security through prohesion offers a troubling vision of the power at work in security surveillance technologies, solace can be found in the fact that this power encounters such difficulty in taking root. Of the three programs examined in this book, one was abolished by the Mexican Senate because of its failings, one is stuck in limbo awaiting action from the Peña Nieto administration, and one is operating in a weakened form that fails to fulfill the vision of automobile security intended in its design. In this sense, weakness is a central aspect of security and prohesion in Mexico.

Failure is a topic that surveillance scholars have treated in the past. The surveillant state has been referred to as the Big Bungler rather than Big Brother, an authority "driven mad by too much power and too much speed."[33] Errors are common in the data that public and private entities gather about us, which "can lead to death in hospitals, stolen elections, and wrongful arrests."[34] The substance of life itself can throw security technologies off. Facial-recognition technologies are doomed to fail "since identity is inherently a hybrid and unstable construct—at the very least, individuals age, take different jobs, acquire and lose credentials, marry and divorce, etc.—it can never be completely and absolutely stabilized."[35] And multiple standards for the recording and storage of information can spoil government attempts to implement a national identity card.[36,c]

But if failure has been recognized in the literature, perhaps it has not received the emphasis it deserves. Within society, we feel either trepidation or relief, depending on our political affiliation, when government designs for surveillance are announced or leaked to the public. And this reveals the confidence we have in these plans. Militarized drones unsettle us because they illustrate how the conduct of warfare and killing is escaping human control and becoming automated. The unimaginably vast snooping activities of the US National Security Agency (NSA) revealed by Edward Snowden, Glenn Greenwald, and Laura Poitras concern the critical minded of us because they imply that the minutiae of our daily phone and electronic communications are open to inspection. The adoption of national identity cards disturbs us because it

[c] These failures have not, however, turned governments off of surveillance technologies. As Clive Norris has noted, "nothing succeeds like failure" when it comes to using technology in the pursuit of security (Norris, "Success of Failure").

signifies the erection of new walls and boundaries that will break our contact with the Other and endanger our free society. In short, our fears about the negative consequences that accompany surveillance technologies rest on the assumption that these technologies have the strength they claim to have. And in the face of this power, as the move to adopt the legal concept of the "right to be forgotten" in the European Union demonstrates, all we as concerned individuals and groups can do is ask that this power be fallible, that it forget.

It is beyond debate that technologies in contemporary society carry a capacity for tracking and oversight unlike anything that has come before. Militarized drones are certainly unleveling the playing field for the conduct of war. NSA surveillance over personal communication, Big Data or otherwise, is an affront to the notion of a free society. Biometric identity cards are a technological step in the direction of increased control over personal identification. And these technologies do sometimes succeed in assassinating suspected terrorists at a distance, scooping up critical pieces of information to stop a crime, or achieving access control. But the continued insecurity of our world speaks to a fundamental weakness or fallibility of security systems.

Perhaps the most telling example in this regard is the Boston Marathon bombings, where the brothers Tamerlan and Dzhokhar Tsarnaev exploded two homemade bombs at the finish line of the foot race on April 15, 2013, killing three and injuring scores of others. Lost in the tragedy of the event and the drama of the subsequent manhunt is the fact that the multiple surveillance programs and various layers of surveillance technologies instituted since the September 11, 2001, terrorist attacks failed to identify the two brothers as threats. This despite the fact that they were born in the conflict-torn Caucasus region of the Soviet Union, self-identified as Chechen, had previous encounters with the police for violent behavior, and learned bomb making from an online magazine published by al-Qaida. What is more, following the attacks, Senators Saxby Chambliss and Richard Burr reported that Russian intelligence officials had warned both the FBI and CIA about the brothers, including recordings of Tamerlan discussing attacks with his mother over the phone.[37] So, then, not only did the "surveillant assemblage" fail to capture these terrorists, but, to invoke a Marxist argument, it might be argued that these technologies have "deskilled" traditional intelligence work to the point where information provided by another country's intelligence service was not acted upon in the manner one might expect.

Similarly, the brothers Cherif and Said Kouachi, who killed twelve and injured eleven during an attack on the offices of the satirical magazine *Charlie Hebdo* in Paris in January 2015, had been under surveillance by French authorities; Cherif had even been arrested and tried on terror charges in 2005 as he was heading to Iraq to fight US forces. Thus, authorities in France, who possess some of most sweeping powers to surveil the public and regularly deport alleged extremists without the procedural protections of the US legal system, were unable to prevent this attack.[38] Zarrar Shah, the technology chief of Lashkar-e-Taiba, the Pakistani terror group that carried out a series of coordinated attacks in Mumbai over the course of three days in November 2008 that left 164 dead and 308 injured, used Google Earth to plot the attacks and was being monitored by British, Indian, and US authorities. Yet, the surveillant assemblage proved too weak to stop these attacks.[39] Ismaaiyl Brinsley, the gunman who ambushed two New York City police officers in December 2014, had earlier in the day shot his girlfriend in Baltimore. Baltimore police, using pinging technology to locate Brinsley's mobile phone, notified New York City police that he was in Brooklyn and was posting messages on his girlfriend's Twitter account saying that he would kill two New York City officers.[40] But this, too, failed to stop the attack. And the events that bookend the birth of the massive US homeland security state—both the September 11, 2001, terrorist attacks and Edward Snowden's whistleblowing about NSA domestic spying—speak to the failure of surveillance. Multiple agencies had information about the September 11 attackers, but this information was not acted upon. And Snowden's revelations demonstrate the permeability of a surveillant assemblage that relies on private firms to provide public security.

Mexico, meanwhile, was rocked in 2014 by the disappearance of the forty-three Rural Teachers' College students in Iguala, Guerrero. A federal investigation implicated the mayor of Iguala and local police. The investigation found that the police had apprehended the students and turned them over to a local crime syndicate, Guerreros Unidos (United Warriors), which then presumably murdered them. Incredibly, despite the immense investment of technology and resources in the fight against crime, the federal government was unable to locate all but one of the students' bodies.

The legality and desirability of intrusive surveillance technologies in our lives will continue to be debated. But if these technologies are already operating, they might be expected to work at least at modest levels. As these examples show, however, security surveillance and prohesion not only sometimes fail but are fundamentally weak forms of protection.

The Registry of Mobile Telephone Users, Citizen Identity Card, and Public Registry of Vehicles pursued by the Calderón administration provide insight into the forces that account for the weakness of the weapons of the security state. First, apart from the technologies themselves, the turn to surveillance technologies speaks to a distinct weakness of government. In Mexico, the state simply cannot govern the way it once did. The elevated levels of ordinary crime, the immense numbers of homicides, the underreported number of femicides, the common kidnappings, and the arms and drugs trafficking all illustrate the inability of the state at both the federal and state levels to provide security.

Chapter 2 discussed the reasons for the weakening of the state and strengthening of criminal elements in Mexico. The dictatorial, single-party rule of the Institutional Revolutionary Party (PRI), whatever its shortcomings as a democratic form of government, provided a centralization of political power that proved able to manage drug trafficking and the violence that can accompany it. Democratization has brought about free, competitive elections at different levels of government and increased civilian control over the political process. But this progress has changed political dynamics in the country, decentralizing power and weakening the clientelist relationships that historically corralled drug violence.[41] At the same time, the death of Amado Carrillo Fuentes, leader of the Juárez cartel, the original *jefe de los jefes* (boss of the bosses), precipitated the current and ongoing wave of violence because it created a power vacuum that various regional cartels and criminal organizations sought to fill. The lack of a monopoly over criminal activities in Mexico by either the state or crime bosses has resulted in a rise of formerly unauthorized forms of violence, such as kidnappings, extortions, and street robberies.[42]

These transformations in Mexico's political landscape were accompanied by changes in the country's economy. The shift from a statist, protectionist economy controlled by the PRI to a neoliberal political economy governed by free-market policies has expanded the gross domestic product and enriched Mexico's upper and upper-middle classes as well as regions along the northern border.[43] But this wealth has not been shared equally; the poverty rate (as measured by income required for basic living expenses) has remained stuck at 50 percent of the population,[44] indicating increasing income inequality. Crime, then, has become one way for people living at the margins of society to pursue economic gain.

Thrown into this social mix is the transformation of Mexican cultural life through exposure to global media, which simultaneously weakens certain forms of traditional national identity while strengthening others—*pulquerías* and *siestas* gradually disappear as tastes and times change in concert with global norms, while *narcocorridos* that glamorize and romanticize the fatalist pursuit of drug wealth rise in popularity as a distinctly Mexican form of cultural expression. Together with an active feminist movement[45] pushing for reproductive rights and other protections, as well as other forms of global consciousness, these changes weaken the legitimacy of traditional authorities and ways of doing things. Thus, over the past decades, the Mexican state has contracted in accordance with the precepts of neoliberal governance, which has reduced its ability to govern, while the society it oversees has continued to expand, evolve, and transform as it absorbs new technologies and means of expression and it experiments with new freedoms presented by democratic governance. With less ability to govern, and an unreliable police force with which such governance could not be entrusted, the Mexican government turned to surveillance technologies as a way to reform itself to govern in a global world.

Second, the national government's failure to fully implement surveillance technologies has shown that it is prone to weakness. Resistance has been central in this regard. Resistance meets authorities' efforts to create the security state at various points. Mobile phone users suspicious of the federal government's registry refused to register their lines honestly. And the poor design of the registry left it unclear how users' phone lines could be verified and who would even have the responsibility for doing so. Drivers unaware or uninterested in the federal government's automobile registry in the states where it was being offered failed to register their vehicles. And many states refused to participate in the program altogether, their reluctance motivated by politics and a fear of wasting precious security resources on a flailing federal program. The Citizen Identity Card failed to launch due to opposition from the government office responsible for issuing a rival identity card.

Resistance is an established topic within surveillance studies. John Gilliom, for instance, in his examination of an electronic payments system that monitors public assistance in Ohio, demonstrates how poor women's defiance of welfare rules constituted an everyday form of resistance that opposed the power of the state as "overseers of the poor."[46]

And Gary T. Marx has provided an authoritative accounting of the myriad ways in which people resist everyday forms of monitoring, such as drug testing in the workplace, a list that includes "refusal" (to take a test), "discovery" (of the date of a random test), "avoidance" (not going to work on testing day), "switching" (a clean drug sample for a tainted one), "distorting" (consuming substances to neutralize the drug test), "masking" (one's identity to testers), and "countersurveillance" (testing on oneself to ensure success)." Marx observes that such strategies "should serve as humbling reminder of need for skepticism in the face of unreflective paranoia and oversold technical surveillance fixes introduced into heterogeneous social contexts."[47]

Supporting Marx's conclusion, the histories of security surveillance in Mexico encourage a broader definition of resistance—any force, whether human or not, that has the effect of obstructing the intended plans and intentions or established relational patterns of authorities (see chapter 4)—to take fuller account of the variety of difficulties inherent in establishing new modes of oversight and governance in society. It is not only that people, whether private citizens, CEOs, or elected officials, oppose these tactics and authorities. But time, space, and the technologies themselves intervene as well. Given these diverse forces, prohesion fails to acquire the power that it was designed to possess.

Implicit in this definition of resistance and central to understanding the weakness of surveillance technologies are the concepts of "distributed agency"[48] and "assemblages"[49] introduced earlier in this work. A car is not simply a car, a phone is not simply a phone, and a person is not simply a person. They are rather elements situated in a larger network of associations between people, organizations, things, and ideas that enliven them. This is "vibrant matter."[50] And having authorities take hold of those things—phones, people, automobiles—in turn means engaging with the range of associations that give them agency. The RENAUT, CEDI, and REPUVE largely failed to take hold of mobile telephony, personal identification, and automobility in Mexico because these collective agencies are distributed across a wide network of users, providers, regulatory agencies, and material things that enables their activity. To get a grasp on mobile telephony, it is not enough to simply have users register their numbers with the appropriate authority. Mobile service providers, the governmental agencies regulating telecommunications, the designers of phones, the placement of cellular towers, and so forth must be integrated into the program as well. To take control of the wheel of automobility, the government must ensure not only that car companies provide records of sales to the government's database and adhere RFID stickers to windshields, but also that state governments and customs officials do the same with vehicles circulating in the country or crossing national borders.

Daniel Neyland, in an innovative examination of governmental efforts to control "everyday objects of terror"—letter bombs, sharp objects and liquids on airplanes, and so on—makes a similar point about the inherent difficulty of securitizing things. "The example of objects in airports," Neyland notes, "suggests that successive actions to build networks of governance around categories of objects (such as liquid containers and sharps), connecting various people (airport managers, passengers, security and check-in staff) and things (boards, plasma screen TVs, leaflets) in order to reorient actions around the object in focus and establish its new ontological status as a matter of concern are messy in practice." Quite simply, he concludes, "it seems that ontologies are stubborn and routinized."[51]

What is most interesting about the ontological stubbornness of things is the manner in which older structures of governance get in the way of newer ones. The principal opposition to the Citizen Identity Card came from the Federal Electoral Institute (IFE). The main challenge to the Public Registry of Vehicles was the opposition or lack of participation of the states. Both the IFE and the federated states of Mexico are bodies that govern in Mexico. Historically, they emerged as authorities worked to solve particular problems of governance that faced the nation. The IFE was created to provide legitimacy to a fledgling democratic electoral system that did not have the trust of the public following the dubious presidential elections of 1988. The states came into existence as a means for governing Mexico's outer territories of that could not be effectively ruled by centralized authorities, giving birth to "the negotiated state."[52] These are state forms that were "co-produced"[53] over time in conjunction with those things and phenomena they were designed to govern. However, the security state encounters them as obstacles that prevent the implementation of prohesion. These thoughts cast in sharper contrast the weakness of weapons whose strength authorities are always assuring us of.

6.4 DETERMINISM AND EMERGENCE

But to say that surveillance technologies are fundamentally weak is not to say that the state in Mexico lacks power. Through these programs, federal authorities can require *sujetos obligados* (obligated subjects) like automobile manufacturers and *entidades federativas* (federated entities) to deliver data about the production, sales, and registration of vehicles to the REPUVE database; local, state, and federal law enforcement use the database to search for and identify stolen vehicles; states such as Sonora are able to employ RFID technology as a tolling solution or the basis for tax collection; and this progress provides the federal government a basis for further extending this surveillant assemblage into other states and state agencies in the future. The federal government has also been able to distribute four million personal identity cards to schoolchildren in several states throughout Mexico. Even with the failed mobile telephone registry, the state was able to register nearly eighty-three million mobile phone numbers, or 90 percent of all numbers in Mexico; and when the registry was ultimately terminated, the federal government succeeded in quickly transferring responsibility for monitoring telecommunications to service providers.

These outcomes and this arrangement of power, however, are not what the state had planned. This is not the secure future that prohesion as a novel form of governmentality promised. It is rather the unexpected result of authorities negotiating with the people, organizations, rules and laws, things, and concepts that had resisted the programs. This arrangement of power is, as noted in the last chapter, the product of statecraft.

The improvisational character of social life has been highlighted by several influential works in the social sciences. The best-known version of this idea is "bricolage," which Claude Lévi-Strauss used to denote tinkering or "someone who works with his hands and uses devious means compared to those of a craftsman"[54] in order to distinguish premodern forms of knowledge from their modern, scientific counterparts.[d] In a

[d] "The bricoleur is adept at performing a large number of diverse tasks," Lévi-Strauss claims, "but, unlike the engineer, he does not subordinate each of them to the availability of raw materials and tools conceived and procured for the purpose of the project. His universe of instruments is closed and the rules of his game are always to make do with 'whatever is at hand'" (Lévi-Strauss, *Savage Mind,* 17). This notion of making do with whatever is at hand has been adapted to a variety of works in the social sciences, perhaps most apropos to the topics discussed here by Claudio Ciborra, an organizational theorist, who in describing the successes and failures of strategic information systems within organizations, comments that "in order to achieve a new SIS (strategic information system) design the issue is neither to try to generate the most creative application idea, nor to realize the design through a careful planning and implementation method. The real issue is being able to overcome those cognitive and institutional barriers that prevent users and designers [from] seeing, appreciating, and utilizing all those potential applications already surrounding the members of an organization" (Ciborra, *Labyrinths of Information,* 44).

similar vein, Andrew Pickering describes scientific and engineering work as "a mangle of practice," a "practical, goal-oriented and goal-revising dialectic of resistance and accommodation" by which scientific knowledge and technological artifacts emerge in time.[55] And most closely related to the current book, James Scott's research on the state argues that state-initiated social-engineering programs, like the collectivization of Soviet farms or the construction of high-modernist cities like Brasilia, are doomed to fail and that human societies would be better served by governance based on "metis," that is, "folk wisdom" or "knowledge that can only come from practical experience."[56]

Recognizing the presence of tinkering and improvisation in the deployment of surveillance technologies has important consequences for understanding the power of the state. Most importantly, it identifies a skill-based, human component of state formation that cannot be reduced to larger structural forces, be they the authority of rulers, the composition of state power, the accumulation of capital, the culture of a society, or the design of technologies. Such forces clearly mattered in the outcomes of the RENAUT, CEDI, and REPUVE. But the successes and failures these programs experienced had as much to do with the skill of state officials and administrators, like Samuel Gallo, in recognizing an opportunity to connect, for example, the REPUVE to an existing state program and negotiate with those authorities to "make things stick."

And to develop the point further, there is nothing—not the skill of the state practitioner, the authority of the lawmaker, the design of the program, the beliefs of the population, the wealth of the company, or anything else—that can guarantee that a particular modification will actually take. In the case of the REPUVE, some improvisations worked. In the case of the RENAUT, most did not, which left monitoring of mobile telephony in Mexico outside the organizational structure of the federal government. The outcomes of the state's adoption of surveillance technologies to fight insecurity are thus decided in good measure through trial and error.

Over the past two decades, there has been increasing acceptance of the idea that social phenomena do not have singular causes but are "co-produced" through the interaction of various elements. The social order is, in other words, emergent. The concept of "emergence," which is central to science and technology studies and "assemblage thinking," offers a needed exit out of the disabling "structure versus agency" debate in the social sciences.[57] Applied to politics, the concept of emergence avoids having to explain the formation of the state as resulting directly from either the plans of great statesmen or the structure of capital, coercion, or culture.[58] As the second chapter illustrated, central dimensions of the Mexican state took shape over time through authorities' evolving efforts to maintain control over communication, identification, and mobility in society. And as the last chapter recounted, even when plans for reforming the state are known in advance, the shape that reform ultimately takes can only be settled in practice.

These ideas are relevant to surveillance studies. Regularly, works on surveillance give the impression that these technologies are transforming the world in line with their technical design. Security as a mode of governance based on the social sort has arisen because electronic identity cards allow biometric data to be stored simultaneously in the cards and government databases. Security is marked by a diminution of democracy because private corporations are intimately involved in the planning, development, and deployment of surveillance systems, and these companies are not accountable to the public as elected officials are. Personal privacy has already passed into history in the surveillance society, because the bits of information that we are constantly generating through our electronic communications, online searches, plastic-card purchases, and so on are scooped up by public agencies and private-sector actors that use the data without our consent. Statements such as these, simplified perhaps but not uncommon, reveal a determinist mode of thinking where direct lines are drawn between particular social phenomena and surveillance technologies, or where the social consequences of surveillance technologies are predicted in advance. This thinking is not technological determinism. It is technology, in conjunction with multinational corporations or secretive state security agencies, that determines outcomes.

It was this tendency toward determinism that prompted thinking about society in terms of emergence in the first place.[e] And remaining

[e] Before "emergence," explanations for the creation of scientific knowledge, technological objects, and their impact on the social world were told in the language of the sociology of scientific knowledge or the social construction of technology. These social constructivist perspectives viewed facts, such as those resulting Robert Boyle's pneumatic experiments (Shapin, "Pump and Circumstance"), and artifacts (Pinch and Bijker, "Social Construction of Facts and Artefacts"), such as the design of bicycles, as the result of cultural forces (the interests of scientists, the creation of dissemination outlets with which to publicize research and widen the witnessing of science, the replication of experiments before influential public figures who could lend increased legitimacy to science, the formation of a particular vocabulary for describing science and demarcating it from other fields of engagement with the natural world believed less rigorous, social mores dictating the propriety of dress for men and women, and so on).

sensitive to emergence is vital, since it can reveal processes of social change and state reformation that surveillance technologies may be creating. With this in mind, a few points on the emergent nature of surveillance technologies are in order.

First, we should expect the unexpected. Surveillance technologies might sometimes function according to design. But they should be expected to morph as the practices of statecraft fit them into particular settings. The REPUVE and the CEDI took root in Mexico, but they did so in forms and with functions distinct from those planned by authorities.

Second, the relevance of things is relative. Certain elements of social arrangements that were once unimportant or nonexistent can become central to the governance of society, while others that were once central can become inconsequential. Programs such as the RENAUT, CEDI, and REPUVE are intended to insert new elements—computer software, biometric identity cards, RFID tags—into existing distributions of collective agency to increase the government's hold over communications, personal identification, and mobility. But statecraft can involve unexpectedly giving new purpose to old elements. State planners used the toll plazas already constructed in Sonora to their advantage in order to install RFID readers to serve the REPUVE program, just as they used public schools throughout the country to register schoolchildren for the CEDI. Statecraft can also involve getting rid of old elements that were once central to the social order. Old laminated cards that people once used for tolls in Sonora are slowly passing out of use. And old elements that were never part of an assemblage to begin with, such as the constitutional right to free transit, which was not being respected in Sonora, can gain new life through the alignment of forces that statecraft and surveillance technologies bring about.

Third, problems can sometimes become solutions. It is interesting to consider how the shape of a particular assemblage can have consequences for its governability. All of the surveillance programs described in this work failed to meet their designs. In the case of the CEDI and REPUVE, the main point of resistance that dogged the programs came from the state itself, from the extant political structure for governing personal identity and automobility in Mexico. The RENAUT, however, encountered no such opposition. A structure of state agencies never coalesced around the mobile phone—a more recent technology that appeared when neoliberal political economy had already made regulation a mostly private affair—as it had around personal identity or the automobile or the land-line phone. Counterintuitively, however, the very political structure that inhibited the implementation of the REPUVE could, because of its permanence, later be recrafted by program administrators to make the program stick. The RENAUT, by contrast, having no existing state structure for program administrators to graft onto, was simply terminated, the responsibility for governance turned over to those in possession of the necessary infrastructure: private service providers.

Finally, as emergent phenomena, security surveillance technologies will take different meanings based on the context into which they are fit. In Sonora, the REPUVE is valued nearly universally as a means for establishing and respecting the right to free transit that was fought for and established in the Mexican Revolution. In Zacatecas, the REPUVE is understood and approached more cautiously as another government program promising security. At border crossings, meanwhile, the REPUVE is viewed negatively as another scheme to squeeze tax revenue out of individuals who import their vehicles from abroad. In sum, what surveillance technologies do and what they mean emerge in time and practice. This is how the power of surveillance technologies forms.

6.5 FATALISM AND ENGAGEMENT

Emergence has surprising political consequences. Thinking about surveillance is often tinged with a dystopian outlook that minimizes the potential of individual and collective action to influence a surveillant assemblage composed of national governments, transnational corporations, and advanced technologies.[59] This skepticism is matched by popular reactions to controversies such as the NSA spying programs, reactions that vary from support (belief that surveillance technologies keep society safe), to indifference (belief that people should have nothing to hide), to impotence (belief that surveillance technologies are invasive but nothing can be done about it).

But the emergent nature of surveillance technologies means that individuals, despite the design of prohesion as a mode of governance that would control society by bypassing people altogether, still influence government in meaningful ways. The lowly bureaucrat plays a key role in tailoring surveillance technologies to fit existing assemblages of collective agency. And ordinary citizens, through organized efforts to resist a phone registry, parental expressions of uneasiness about the collection of schoolchildren's biometric data, or mere gossiping about state surveillance, help determine whether and how these efforts stick.

If ordinary people remain central to the outcomes of surveillance technologies in society, what are we to do? Which types of actions might influence the presence of surveillance technologies in our lives? How might "participatory democracy [be] enacted through work in and on material objects" such as surveillance technologies?[60]

A sensible place to begin answering these questions is with the efforts activists are already making to engage the surveillant assemblage. Here, it is appropriate to mention the whistleblowers in the employ of the national security state—Chelsea Manning and Edward Snowden—who brought attention to the operation and scale of state security surveillance by releasing classified information about their work. The actions of these individuals, undertaken with the assumption that their lives would be destroyed, were brave and daring. And they resulted in public awareness about the abuses of the US national security state, an essential first step to broader action.[f] Increasing awareness about the workings of surveillance in the world today is the goal of a wider network of activists as well, including the more academically minded Surveillance Studies Centre housed at Queen's University in Canada and civil liberties organizations such as the Electronic Frontier Foundation and the Electronic Privacy Information Center. These groups have organized to pass key legislation or support litigation establishing individual rights against state surveillance. Representative of this collective labor is the "right to be forgotten" established by the European Court of Justice. The court's ruling in *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos, Mario Costeja González* provides all individuals in Europe the right to prohibit Google and other search engines from linking to items that are "inadequate, irrelevant or no longer relevant, or excessive in relation to the purposes for which they were processed and in the light of the time that has elapsed."[61]

Efforts such as these concern the encroachment of surveillance on fundamental civil liberties. Generally, the surveillance in question is undertaken in the name of national security or by companies involved in information commerce. Such efforts, then, resemble the organized

[f] Indeed, in the wake of the Snowden disclosures, the US Congress decided to phase out the NSA's bulk collection of phone records, and allies of the United States subject to its surveillance have drafted resolutions in the United Nations calling for a cessation of such surveillance.

resistance to state surveillance described in this book, such as the digital mobilization of phone users in Mexico against the RENAUT and the subsequent campaigns against Peña Nieto's telecommunications reform, which activists saw as a threat to net neutrality. Taken together, individuals in these instances can be seen working to ensure *freedom*—to preserve a free space in society unfettered by surveillance technologies, which is a condition for democracy.

These efforts, though, assume that surveillance is unsuitable to any civic purpose. This might seem like a trivial qualification, since the massive sweep of information that takes place under the NSA's domestic surveillance program so clearly violates our sense of basic decency and liberty. But there are many examples in which activists have worked to extend the surveillant power of the state to areas of social life often kept in the dark. A clear example is gender violence, such as intimate partner abuse and sexual assaults, where offenders are enabled by the deference the state has historically paid to family privacy and by the stigma of being a victim of such crimes. While legal measures have been passed to protect women from physical and sexual abuse, the power of such laws often proves ineffective against assailants unafraid of criminal sanction. In response, antiviolence advocates across the United States, for instance, have campaigned for legislation that would establish monitoring programs featuring GPS technology to track abusers who repeatedly violate restraining orders and would alert victims when they are nearby.[62] Using surveillance technology to confront gender violence is relevant to Mexico too, where femicides are a prominent form of crime. To combat them, activists have advocated for the use of information technology and mobile devices to publicize the problem and give potential victims the ability to access help.[63]

As these examples illustrate, the situations where activists might campaign for more state surveillance often involve crime rather than national security or data commercialization. In these instances, people look to extend the surveillant power of the state to provide the protection of the law to individuals who are not receiving it. But like the examples of national security and data commercialization, it is assumed that a rule of law exists in society and that authorities have an interest in extending surveillance.[g]

[g] It should be noted that in Mexico, women's advocates have often accused the government of apathy toward victims of femicides.

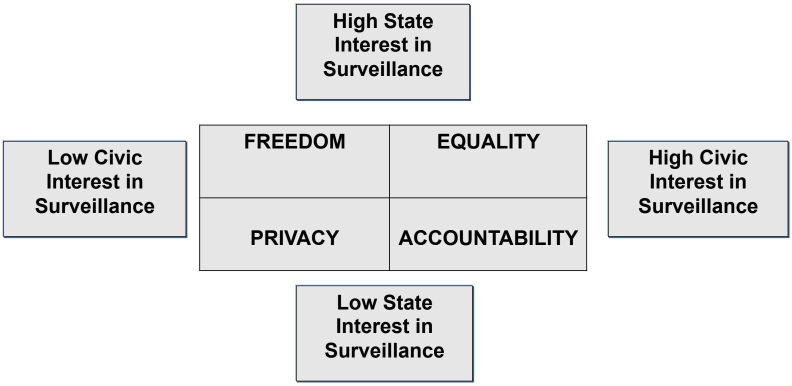
High State Interest in Surveillance
Low Civic Interest in Surveillance
FREEDOM
EQUALITY
PRIVACY
ACCOUNTABILITY
High Civic Interest in Surveillance
Low State Interest in Surveillance

FIGURE 26. Values at stake in surveillance politics.

These considerations help mark out a pair of axes—civic interest in surveillance and state interest in surveillance—against which a politics of surveillance can be measured. Where civic interest in surveillance is low but state interest high, as in the cases of national security and data commerce, activism can be thought to concern *freedom*. Where civic interest in surveillance is high and state interest is too, as in the case of gender violence, activism can be thought to concern *equality*. Those working to end gender violence are interested in ensuring women equal protection before the law (fig. 26).

Campaigns centered around equality reflect what David Lyon has referred to as the "care" dimension of surveillance technologies, at work in hospitals and schools, that accompanies the more discussed "control" dimension. Such campaigns also embody his call for surveillance governed "by an ontology of peace rather than of violence" and "an ethic of care rather than control."[64] They also relate to the "conviviality" of technology that Torin Monahan has called for, describing technologies that "not only afford but also invite modification on the part of users, support diverse modes of expression, and enable power equalization among people."[65]

In contrast to the scenarios involving national security and crime, where state interest in surveillance is a constant, there are others where it is not. In New York City, for instance, public outcry over the conduct of its police force, including the disproportionate use of stop-and-frisk tactics on poor and racial and ethnic minorities, pushed Mayor Bill de Blasio and Police Commissioner William Bratton to implement a pilot program in which police officers wear body cameras to monitor their interactions with the public.[66] While unpopular with the officers, who contend that the cameras will deter people from wanting to talk to them and violate their privacy,[67] police use of such body cameras is expanding in the United States. At the national security level, the US War on Terror has been conducted in a shadowy realm—involving extralegal tactics such as extraordinary rendition, black sites, and secret intelligence court rulings—that activists seek to bring to light.

In these instances, authorities engage in violence—police use of excessive or illegitimate force, the CIA abduction of terror suspects—that they wish to keep from public view. Against these machinations of power, activists use surveillance technologies—body cameras, flight records, maps—to document the illicit actions of the state. In contrast to subjects concerned with *freedom,* who use the rule of law to oppose the state's expansion of surveillance, and subjects concerned with *equality,* who use the rule of law to support the state's expansion of surveillance, individuals here find themselves without a true rule of law. In these settings, they use surveillance technologies to foster *accountability* and legality.

This politically progressive use of surveillance technologies has been pursued by activists in Mexico to document and publicize the assassination of journalists. The map and accompanying database assembled through the Mi México Transparente (My Transparent Mexico) project provides a register of the number and type of attacks suffered by journalists.[68] This register functions as an ongoing surveillant document that announces the threat faced by journalists to members of the state and criminal community who might prefer to silence reporting.

Another innovative use of surveillance technology involved the Yo Soy 132 (I Am 132) movement that captured international attention in 2012 during Enrique Peña Nieto's presidential campaign. In May 2012, the then PRI candidate presented his political platform at the prestigious Ibero-American University, in the prosperous Santa Fe area of Mexico City. During the question and answer session, Peña Nieto angered students when he aggressively defended his actions as governor of the state of Mexico in the 2006 Atenco case, in which hundreds of state police were sent to break up a protest against the planned construction of a new airport. During the police action, two hundred activists were arrested, two were killed, and twenty-six women were sexually assaulted.[69] Following the candidate's response, students broke out with chants of "Assassin!" and "Get out!"

Media coverage of the event downplayed the protest by attributing it to elements outside the university rather than Ibero students, members of one of the more respected institutions in Mexico. Responding to what they saw as the media's attempt to appease the popular candidate's political camp, 131 Ibero students produced a YouTube video showing them with their identity cards as a way of documenting their status as Ibero students and their opposition to Peña Nieto. The video went viral. And supporters of the students responded on Twitter by announcing "Yo Soy 132," or "I am 132," adding themselves to the list of young people against the candidate. Thus, against a media and political establishment that dismissed dissenting voices as disreputable malcontents not worthy of society's respect, the Ibero students and their supporters used the tools of surveillance to announce their presence and opposition to authorities.

Finally, in addition to activists who oppose the state's support of surveillance in pursuit of *freedom,* activists who endorse the state's support of surveillance to fight for *equality,* and activists who support surveillance against the state for *accountability,* it stands to reason that there are contexts in which neither the public nor the state have an interest in surveillance, or at least an interest that would support democratic ideals. This raises what can be called a true sphere of *personal privacy,* where the details of the nonpublic lives of both governors and governed would be respected and not subject to surveillance. The sexual liaisons of public officials (US president Bill Clinton or French president François Hollande come to mind, assuming no crimes were involved) or other details of public leaders' personal lives could be imagined as of no significance for the welfare of the country. And the same assumptions could be made of the intimate personal details of citizens' lives. The fact that there is knowledge about public officials' personal lives or that the state surveils personal aspects of citizen's lives indicates a certain perversion of democratic ideals that has come to masquerade as political controversy.

Nowhere is this more apparent than in the political battles over reproductive rights. The steady push to criminalize abortion in those countries where it is protected under law functions as an effort to increase control over the private lives of women, serving in turn to diminish their capacity to be full subjects in society. And surveillance plays a central role in this contest. The US state of Indiana, for instance, recently considered, although ultimately did not pass, a measure that would have required doctors to partner with and publicize the names of other medical professionals—"backup doctors"—who might treat any complications or emergencies related to an abortion in a nearby hospital. Through such legislation, antiabortion activists sought to publicize the names of doctors who perform abortions, which would presumably expose them to intimidation.[70]

Surveillance over people's personal lives works to the detriment of democratic governance. In these contexts, then, efforts to protect women's right to control their own bodies or to establish that right where it does not exist count as political actions in support of subjecthood. In this regard, the movement to decriminalize abortions in Mexico can be understood as not only an extension of women's rights but also the creation of a social and legal notion of personal privacy that is critical to democracy.

This description of the differing relationships between subjects and surveillance in democratic society is surely too neat. The categories overlap in practice. Many citizens express no concern that surveillance in the name of national security infringes on basic liberties and freedoms. Others would be opposed to the expansion of surveillance in the name of crime fighting, even to combat gender violence, since it would invariably encroach on a sphere of life thought private. Many people consider government secrecy in policing, intelligence, and warfare critical to security. And others believe that freedom of speech provides the legal justification for peering into the private details of people's lives. Quite simply, not all people are the same, nor are all governments the same when it comes to surveillance.[71] But the purpose of this thought exercise is not to close the door to thinking about surveillance technologies, but to open it in order to think about them differently in the hope that they might effect a wider change in how we interact with authorities.

With this in mind, we might return to El Bunker and consider again the architectures of authority found around Mexico City's Chapultepec Park. The subterranean Federal Police Intelligence Center serves as an apt symbol for contemporary approaches to security governance. It operates out of view of ordinary citizens while attempting to remain in contact with them through its array of advanced surveillance technologies. And its technical struggles prove equally emblematic of the failings of this strategy. Historical data are unmanageable, interagency communications are unreliable, state agencies are reluctant to share data, and manual processes of information management at the local level slow data processing and accuracy. It is doubtful that constructing more bunkers will prove decisive in Mexico's War on Crime. If building edifices like Chapultepec Castle above the people bore little fruit in terms of achieving a better society, it should not be surprising that constructing fortresses like El Bunker below them should prove disappointing as well. Only by building structures that require those in positions of power to see eye to eye with those in whose name they govern can a more just and secure future be brought into view.