28

The uncertainty principle

Qualification, contingency and fluidity in technology and social control

Gary T. Marx and Keith Guzik

Odysseus and the seduction of technological certainty

In the *Iliad*, Homer recounts Odysseus' control efforts to avoid hearing the dangerous song of the Sirens. As Odysseus approached the island of the Sirens, he reports,

> I … sliced a large cake of beeswax with my sword-edge, and kneaded the slivers in my strong hands until the pressure and the rays of Lord Helios Hyperion heated it. Then I plugged the ears of each of my friends, and they tied me hand and foot and stood me upright in the mast housing, and fastened the rope ends round the mast itself. Then sitting down again, they struck the grey water with their oars … when we were within hail of the shore, the Sirens could not fail to see our speeding vessel, and began their clear singing:
>
> 'Famous Odysseus, great glory of Achaea, draw near, and bring your ship to rest, and listen to our voices. No man rows past this isle in his dark ship without hearing the honeysweet sound from our lips.'
>
> This was the haunting song the Sirens sang, and I longed to listen, commanding my crew by my expression to set me free. But they bent to their oars and rowed harder, tightened my bonds and added more rope. Not till they had rowed beyond the Sirens, so we no longer heard their voices and song, did my loyal friends clear the wax that plugged their ears, and untie me.
>
> *(Homer,* The Odyssey*, Book XII: 165–200)*

Odysseus knows he must resist the Sirens' song and he also knows that he will be unable to resist temptation without a strategy of mechanical intervention. Hence ears are plugged and he is tied until safely beyond their range. For Homer, Odysseus's passing of the Sirens exemplified the cleverness and guile central to Greek notions of heroism. For Horkheimer and Adorno (1972 [1944]), meanwhile, the tale spoke to the deep historical roots of the social inequalities exacerbated by modern industrial society. Odysseus, by commanding his charges to block their ears and fasten him to the ship's mast, ensures the safety of the vessel, all while denying them and reserving for himself the pleasure of the Sirens' song.

For the purposes of this chapter, the story speaks to society's faith in mechanical solutions to problems. Through the proper technological intervention, in this case blocking communication and preventing physical movement, danger can be avoided. Moving right along, several thousand years later, have you ever encountered a web site that would not let you access it unless you entered a valid email address and a password with at least 8 small and capital letters and at least one number? Or what about a bathroom with cameras and biometric access that also measures outputs? (see Appendix A – "Raising Your Hand Just Won't Do.") The preventive efforts of both Odysseus and more contemporary examples nicely illustrate this chapter's topic of the use of technology for social control.

Today, political leaders, bosses, and other authorities promise that the ever expanding repertoire of communication and information technologies (when subject to appropriate controls as decided by them) will better secure society and keep the ship steady. People today are flooded with communication rather than being blocked from it as with Odysseus's sailors. This leaves us to wonder what risks we may face as authorities seek ever greater access to our songs, even as they may restrict or softly manage our access to theirs.

The historical and cultural roots of technology as social control trace back far beyond the Greeks' use of the word *techne* to mean practical skill. But what do the terms social control and technology mean today? Traditionally social control referred to the integration or meshing of institutions such as the family, education, religion, work and government (Janowitz 1975; Gibbs 1989). This approach looks at the total society, the largely unplanned factors in its evolution and the ways, and extent to which, the parts mesh in providing social guidance and order. In contrast, contemporary social scientists use the term to refer more directly to behavior that involves rules and standards – their creation, mechanisms for conformity, the discovery of violations and violators, and processes of adjudication and sanctioning.

Control or enforcement through material technology, the emphasis of this chapter, is only one of many control modalities intended to create rule adherence. Other related forms are socialization, appeals to conscience and reason, peer pressure, informing, licenses and bonds and insurance, rewards and punishments, habit and repetition, exclusion and inclusion and deception and manipulation. The relative importance of these varies across time periods, types of rule and violation, setting and actor involved, but as this handbook demonstrates, the *engineering of social control* is a defining characteristic of modern society and almost always has a seat at the table. It is so prominent, ubiquitous, and transparent in daily life that it is often taken for granted. Our personal, spatial, communication, social, cultural, and psychological environments and borders are increasingly subject to technological strategies designed to influence behavior, whether involving conformity with rules, safety, consumption, or attitudes. The communication and information technologies at the heart of the computing revolution are touted as possessing near magical powers that will allow social control, and hence security and other benefits.

As Cole's contribution to this volume (Chapter 29) illustrates, DNA identification represents the latest in a long line of technologies (fingerprinting, lie detector tests, etc.) that were purported to offer the police "material objectivity" in identifying criminal offenders. Green technologies promise consumers the comforts of modern living (clean water, automobiles) without the harmful side-effects that industrial life wrought (polluted water, poisonous car emissions) (see Brisman and South, Chapter 18, this volume). Algorithms offer the potential of better decision-making on vital economic and planning matters without the error of human actors (see Pagallo, Chapter 37, this volume).

Marx (2016) asks if we are becoming a *maximum security society* in noting the increased parallels between the highly rationalized social control of the maximum security prison and control efforts seen in the broader *surveillance society*. Such a society is ever more transparent, porous and regulated, as the traditional borders that formerly protected personal information and choice are weakened or obliterated by new technologies, new ways of living, and new threats. Control is ubiquitous, varied and integrated into networks of astounding complexity.

The maximum security society is reflected in eleven sub-societies: A *hard-engineered* society where control is sought via materially altering the environment; a seductive and *soft engineered* society relying on persuasion, invisibility and deception; a *dossier* society based on extensive record keeping; an *actuarial* society based on predictive statistics; a *transparent* society where ever more aspects of life are visible to authorities; a *self-monitored* society relying on self-control as a result of measurements and education; a *suspicious* society expecting people to prove that they are innocent; a *networked* society of ambient and ubiquitous sensors in constant communication; a *safe and secure* society with attenuated tolerance for risk; a "*who are you?*" society of protean identities both asserted by, and imposed upon, individuals; a "*where are you, where have you been, who else is there, and what did you do?*" society of mobility and location documentation.

These efforts at rational control involve varying degrees of generality. This chapter deals with the broadest forms – -the hard and soft engineered societies within which the others nestle and twirl. The use of science-based technology to control and influence persons is central to modernization, whether for purposes of crime control in the form of "hard" prevention or "soft" intelligence/information collection and communication for risk management and influence – whether to sell toothpaste or candidates for office or to stop drugs through "just say no" campaigns.

But, as this chapter argues, control often evades the grasp of the engineers and entrepreneurs (whether economic or moral) who tout such technologies as the easy answer to problems of security and public safety. In contrast, this article develops the idea of the *uncertainty principle* as applied to the outcomes of surveillance technologies (although it also applies to other social control efforts). To get there, concepts need to be defined and surveillance as a form of the *engineering of control* connected to other aspects of control. To do that, the next section suggests a language to organize and contrast the array of contemporary control technologies. The major kinds and sources of variation will be identified before turning to empirical inquiry. We then consider a single case study of a Mexican government effort to monitor automobiles for the purposes of public security. We do this to highlight some of the obstacles facing social control through technology. The chapter then ends with a description of the *uncertainty principle* that sets the stage for further inquiries into the uncertainty and unpredictability of the rapidly expanding hard engineering of social control that so defines our age.

Technology and social control: variables and definitions

Considerable variability is found in traditional definitions of technology in the social sciences. For Karl Marx, technology is a key element in the historical movement from feudal, trade-oriented, and early manufacturing society to industrial society. Technological artifacts are central to the economy (Marx 1947, 1956). Critical here is the ideal of technology as a self-realizing, self-defining activity through which humans "begin to distinguish themselves from animals as soon as they begin to produce their means of subsistence" (Tucker 1978). For Weber, technology figures not as productive activity, nor as artifact, but as a mode of thinking and acting in and on the world, "the application of the (technically) most efficient means to given ends within the various spheres of social life" (Schroeder 1995: 228). But more generally, we can define technology as the strategic application of means to ends, whether or not there is a material component, as Karl Marx would have it, or the effort "works" in a literal sense, as Weber stresses. Lip, eye and facial reading for example are technologies because they involve an intentional application of a means to an end, so too does the technology of the rain dance, even though none of them have a material base. It is important to analyze the consequences of the presence or absence of a tangible tool, what it means to say something "works," and whether an outcome can be scientifically accounted for. But neither materiality nor effectiveness are defining characteristics of technology per se.

Another way of defining technology is to see its role in *extending* human capability and resistance (Brey, Chapter 1, this volume), a more practice-oriented view that reflects Marxist emphasis on human labor and intentionality. The use of animals, steam, combustion, electricity, nuclear, wind and solar technologies extend innate abilities, as do sling shots, guns and missiles and hydraulic lifts and robots. Similarly, new surveillance tools that extend the senses (e.g. seeing in the dark or from outer space), or tools offering remote communication and control illustrate this. Computers expand information capabilities regarding both the amount of information available and the ability to store, analyze and share it.

While the effort to extend human ability is a driving force in invention, we can also note efforts to diminish that ability. Some technologies are designed for *eliminating, blocking* or *impeding*, rather than extending, human capabilities (at least on the part of potential rule breakers). The engineering of control may involve *target hardening* or *suspect softening*. Such actions are intended to make it impossible, or much more difficult, for offenders (although it leaves untouched motivation). Examples of hardening can be seen in the moats and formidable walls of the fortress, in the protection of the closed door (whether locked or unlocked), in titanium locks for bicycles, in biometric controls on cars or weapons that restrict use to registered persons, and in encryption or passwords that block access to information. Examples of suspect softening include castrating sex offenders and Antabuse for alcoholism.

These ideas can be related to the *extensive perspective* on technology. They call attention to the interactional and hierarchical dimensions of technology employed for social control. The efforts of one person to extend their capabilities by restricting access through *target hardening* (say, the titanium lock on the bicycle) come at the expense of others' attempts to extend their capabilities by acquiring that target (the bicycle itself).

To deepen the distinction between *target hardening* and *suspect softening*, we can also say that the hard-edges of preventive means seek to bypass the will of the suspect, leaving the individual little choice but to conform or, if violation remains possible, to face increased risks. Contrast a high wall embedded with broken glass encircling the perimeter of a property with encirclement by a low hedge that permits trespassing by simply climbing over it. The hedge is a symbol communicating to the potential trespasser that this is private property, even as the choice to enter it remains. That isn't the case (or isn't the case without neutralization actions and risk) for the high wall. Engineering solutions such as the high wall or high voltage electrified fence (that bootlegs in punishment as well as exclusion) are presumed to offer more security. Of course, the low hedge could offer that as well by the presence of snarling guard dogs wearing video-cams, even though trespassing in principle remains possible.

There is an ethos of certainty associated with hard engineering solutions. This is expressed by what the head of a large corporation said (in a satirical statement which could almost be true) about his company's automated toilets. These were engineered to serve goals of work productivity, health and crime control. He said, "we believe that our trusted employees will do the right thing when given no other choice" (see Appendix A). This statement reflects the effort to eliminate the possibility of making bad choices through hard-engineering.

The view contrasts with the soft-edges of other control means, which are based on the premise (or hope) that violators are rational beings whose behavior will be governed by consideration of the imagined consequences of a given line of behavior. Deterrence may be sought from lessening or eliminating the value of objects that can be stolen. Consider a bank's marked money attached to a hidden, exploding dye packet; or indelible serial numbers on property. Another means is to block the access that potential suspects have to a resource needed for the violation, such as weapons or chemicals needed to make drugs or explosives. Drug treatment interventions intended to convince or teach someone that they do not really need or value the thing they desire are another example.

Dossiers and actuarial data, although dependent on passive sensors and computers, are soft discretionary tools intended to also shape the choices of individuals – both agents of control and potential offenders. Algorithms used by authorities for profiling are intended to manage criminal justice decisions. Information about engineered controls is communicated to potential violators in the hope that they will self-regulate after assessing the likely consequences. This can involve realizing that carrying out the offense is impossible or that, while possible to literally carry it out, the risks of identification and apprehension are too great, not to mention the other costs, such as bodily harm from climbing a barbed wire or electrified fence.

Our discussion has noted factors such as goals (prevention, deterrence, identification); focus (subject, resources used in violation, objects sought such as money or information); and type of offense (theft, violation of trust, contraband, violence). As these factors illustrate, there is a clear variability and complexity at play when we talk about technology and social control. To systematize this further, we can offer seven ideal types that vary in social control and technology settings.

1. Target strengthening and insulation

This is an ancient technique in which the victim or object of desire remains but is protected. Perimeter maintaining strategies such as gated communities, fences, guards, and dogs can be distinguished from more specific protections surrounding an object such as safes, armor, chastity belts, and goods in locked cases or chained to immovable objects. The architectural development of "skywalks" linking downtown private buildings creates "sanitary zones" more subject to control than the potentially disorderly public streets below. Targets may be insulated in a different sense by being hidden or disguised. Pagallo's work in this volume (Chapter 37) suggests that websites can be insulated from malicious robots by requiring a human user to type in dancing letters at a prompt in order to gain access to them.

2. Target or facility removal

This reflects the logic of hard prevention. Something that is not there cannot be taken or used. The move toward a cashless society is one example. Merchants who only accept credit or debit cards, or whose registers never have more than a modest amount of cash in them, are unlikely to be robbed by conventional means. Furniture built into the wall cannot be stolen. Subway cars and buses made with graffiti resistant metals are hard to draw upon. Such strategies can also focus on removing objects from society thought harmful, such as illegally cultivated marijuana (Schuilenburg 2015) or automobiles running on fossil fuels (Brisman and South, Chapter 18, this volume).

3. Target devaluation

This lessens or eliminates the value of what is sought. The object remains, but its uselessness makes it unattractive. Examples include products that self-destruct, as with some car radios when stolen or mixing a bad smelling chemical into a product to work against it being inhaled for its hallucinatory effects and biometric and encryption controls on computers and other goods. To preview the empirical case study in the next section, Mexican authorities have recently attempted to combat stolen mobile phones and automobiles used in kidnappings and drug trafficking by registering all phones and automobiles with the state – thus, a stolen unit would be reported as stolen and lose its value (Guzik 2016).

A concept cutting across the three above is *resilience*. As a strategy, it starts with the assumption that stuff will always happen in a complex and complicated world. Under such conditions, the question becomes how can society best respond to and limit harm, rather than trying to prevent things that cannot be prevented or necessarily anticipated. Thus the Internet with its hydra headed, decentralized structure was created to resist an attack on a centralized structure. Environmental restrictions about building on flood planes or using floating foundations are ways of overcoming tidal waves and resisting earthquakes. A European Union project (IRISS 2014) applies the concept to surveillance societies.

4. Offence/offender/target identification

These strategies are present when it is not possible to physically prevent the violation, or where it is too expensive to do so. A focus on surveillance, technology and social control is most prominent here. The goal is to discover the violation or problem and various details such as how it was done, where contraband is, who is responsible and where the responsible person(s) or group(s) or object(s) are and if a transaction is legitimate. These can also serve as victim warnings. A major goal of nineteenth-century forensic science was to develop biometric measures of identity based on the analysis of fingerprints, facial measurements, mug shots, and chemical properties (Thorwald 1965; Cole, this volume). These have significantly expanded from involving a person's gait and voice to tracking their distinctive smell and internet searches. Electronic monitoring or location devices based on GPS are other contemporary examples. Mexico's REPUVE program (discussed in the next section), involves vehicle registration and tracking. And national ID cards (Guzik 2016; Breckenridge 2014; Lyon 2009) would serve to identify all persons in order to facilitate the identification of criminal offenders after the fact. Or consider an effort to help save endangered species such as Mountain Gorillas or to warn villagers when a dangerous elephant is approaching by attaching collars that ping to iPhones (Ozy 2016).

5. Offender weakening or incapacitation

This seeks to render potential offenders harmless by disabling or weakening their will or ability to violate the norm in question. The means may act directly on the body such as cutting off the hands of thieves or lowering serotonin levels to curb violence, or the focus may be on the mind as with aversion therapy. Various citizen protection devices that can be defensively used, such as mace, fit here, as do non-lethal crowd control devices such as electrical, chemical, strobe, and acoustical immobilizers that disorient, stop, restrain, or block individuals.

6. Exclusion

This seeks to keep potential offenders away from targets or tempting environments by banning them from certain places or activities, such as requiring badges and passwords to enter secure sites, excluding minors from bars, curfews, and even exile and related forms of segregation as with prisons. Capital punishment is the ultimate fail-safe form of exclusionary social control.

With the human genome project completed, neo-eugenic modes of exclusion are likely to be advocated, avoiding the uncomfortable task of the state putting people to death. We are also likely to see new restrictions on those deemed to be genetically at risk of violent and other anti-social behavior. Banning identified card counters from casinos or shoplifters from a store are intended to function as exclusion of offenders from privileged sites of commerce (Schuilenburg 2015).

7. Victim warning

This involves altering the material world such that those who might be harmed are alerted to an impending risk, as with elephants wearing electronic collars. A broken tamper-proof seal or failure to hear a popping sound on food products is intended to alert the user that all might not be well. The visible warning offered by branding or clipping the ears of convicts found in medieval Europe offers another example, while the stigma might serve to deter others from being labeled.

These ideal types help us conceptualize the various ways authorities and individuals use social control technologies, whether with respect to public safety or individuals securing valuable items. And they can be applied to help conceptualize different empirical programs and strategies. They also provide a launch point for considering the main substance of this chapter, the not infrequent failure of such strategies to reach their goals. As recent work (Guzik 2016; Schuilenburg 2015; Breckenridge 2014) illustrates, uncertainty is inherent to technology and social control. In Mexico, the state surveillance programs that involved surveillance technologies to create a national registry of mobile devices and automobiles (*target identification* and *target devaluation*) struggled to get off the ground, with the former being terminated before it could be fixed and the latter being transformed and operational in only a few parts of the country. In South Africa, the effort to launch a national ID card (*offender identification*) failed and had to be cancelled (Breckenridge 2014). The various projects studied by Schuilenburg in the Netherlands – marijuana eradication (*target/facility removal*), road transport policing (*target identification*), and shop bans (*exlusion*) – faced various challenges and proved a disappointment to policymakers and officials working with them. The "truth machines" described by Cole (this volume), which are meant to realize *offender identification*, have each failed to live up to their hype.

The reasons behind such struggles are diverse, reflecting the complexity of the social control relationships into which technologies are embedded. To illustrate this complexity, the next section describes a state surveillance program based on technology to fight vehicular crime in Mexico. The case study that follows documents many of the basic factors associated with the uncertainty of technologized social control.

Mexico's public registry of vehicles: a case study in uncertainty

On June 22, 2009, Mexican President Felipe Calderón inaugurated the Public Registry of Vehicles (REPUVE) by placing the program's first radio-frequency identification (RFID) sticker on the inside windshield of a Chevrolet Suburban at a toll booth outside Mexico City. The REPUVE was designed to do three things: (1) create a centralized federal registry of all cars circulating in the country, including vehicle identification number, registration information, physical description, and the name and address of owners; (2) attach 18000-C type RFID tags onto vehicles containing the unit's registration details; and (3) install RFID readers and license plate recognition (LPR) cameras at transit points across the country to verify the status of passing vehicles. In doing this, the registry would serve as a tool to combat crimes involving automobiles, including car thefts, kidnappings, and drug trafficking. The program thus represents a critical tool in the state's fight against organized crime.

The REPUVE database is administered by the Executive Secretary for the National System of Public Security (SESNSP) and receives data from three separate types of sources: "federal authorities" (federal agencies such as the Secretariat of Finance and Public Credit, which manages customs in Mexico); "federative entities," (state-level agencies such as departments of motor vehicles); and "obligated subjects" (private sector businesses dealing with automobiles, such as manufacturers, importers, financing agencies, and insurance companies). Any person can consult the REPUVE database (via a web interface) for information on vehicles, which allows them to know whether the vehicle they own or are acquiring/selling had previously been stolen.

The RFID tags featured in the REPUVE program, produced by the Neology Corporation, contain a microchip that can store 800 bits of information and transmit that data via radio frequency. As passive tags, the RFID stickers only transmit data upon being activated by a RFID reader. The tags are not applied to vehicles by the SESNSP, but are distributed to the "federal authorities", "federative entities," and "obligated subjects", who are responsible for applying them. In the case of new vehicles, the "obligated subjects" who produce or import them simply record VINs onto the chips, adhere the chips onto vehicles, and then report the link between the VINS and chips into the REPUVE database. In the case of cars already circulating, "federal authorities" and "federative entities" apply the RFID tags following a physical inspection of vehicles and corresponding documents.

While a critical piece of Mexico's anti-crime fight, the REPUVE experienced problems soon after its launch. First, although the program was designed to have all of the nearly 25 million vehicles circulating in the country registered with RFID tags by 2012, less than half of Mexico's 32 states were actually applying them to vehicles as that deadline approached. Second, where the registry was functioning, it was not necessarily doing so as a solution to insecurity, but as a solution for highway tolling and customs inspections at the border. Thus, despite the design of the program to serve as a tool that federal authorities in Mexico would wield in order to achieve target hardening and target identification, the REPUVE has struggled to meet this purpose. It thus serves as an ideal case study of the uncertainty surrounding surveillance technologies and social control.

So, what accounts for the uncertainty experienced by the REPUVE? In the remainder of this section, we cover seven basic factors that are essential for understanding the way the REPUVE, and social control efforts more generally, develop. These are: (1) the goals of agents; (2) the interests of organizations; (3) political and legal settings; (4) the resistance of subjects; (5) cultural contexts; (6) material tools and objects; and (7) geography and space.

1. Agents and goals

In other work, Marx (2016) offers a description of the structures undergirding surveillance and other types of social control, a truncated list of which includes *agents* (those who conduct surveillance), *subjects* (those who are surveilled), *audience* (those for whom surveillance is conducted or who otherwise observe it), and *organizations* (whether surveillance takes place within an organizational setting/by an organization or not). By definition, one goal of an agent of social control is to collect data on subjects. In the case of REPUVE, as in many social control operations, monitoring is distributed across multiple actors. These include, but are not limited to, the federal employees within the SESNSP, which oversees the program and its database; the state-level technicians and administrators at registration sites, who inspect vehicles already on the road, place tags on them, and then feed their data into the REPUVE database; and the private technicians working within car producers and importers, who apply tags to new vehicles they produce and share the information with the REPUVE database.

Shared labor does not mean however that control agents share the same goals. For instance, the SESNSP can be seen to possess multiple goals in gathering data for the program. Above all, it wants the compliance of drivers, businesses, and states with the REPUVE law. Compliance is demonstrated, in turn, through records of inspections and registrations of vehicles by companies (in the case of new vehicles) and by state inspectors (in the case of used vehicles). But it is looking to make this information public in order to help citizens make more informed decisions about car purchases. And since the REPUVE is a federal program that could be cancelled by an incoming presidential administration, the SESNSP is also looking to ensure the program's continuity, lest it be cancelled. Thus, monitoring activities serve not only to fulfil the law and fight crime, but to illustrate the program's progress to the public and ensure its own survival amidst political turnover.

The other agents, meanwhile, the state-level technicians and administrators and the private companies, possess goals beyond collecting and sharing data on registered vehicles to the REPUVE database. At the state level, data gathering is conducted by agents and administrators from finance ministries or attorney generals' offices. And collecting vehicular data can not only serve the REPUVE database, but also taxation applications as well. Conversely, attorney generals' offices overwhelmed with other security concerns, of which there are many in Mexico, might be less invested in data collection on vehicles.

With private sector agents, a similar multiplicity of goals is present. Their main concern is profit. Thus, companies collect and report data in order to be in compliance with the REPUVE law and not expose themselves to fines and sanctions. But companies might also see participation and collection of data and placement of tags as a competitive advantage, which will make their vehicles appear safer and thus more desirable to purchasers. Conversely, if the expenses of participating in the program are too great, they might oppose participating altogether.

So, the structure of social control is distributed across various actors. And to the extent that the goals of different agents coincide, the activity can be expected to conform to a greater degree to expectations and plans for that program. But to the extent that goals of different agents do not coincide, then the outcomes of the activity can be expected to not conform to expectations.

2. Organizations and interests

The preceding points illustrate that in considering the goals of different surveillance agents, we need remain aware of the organizations involved in that control activity (Marx 2016). Individual efforts to control, because they are solitary, are distinct from the efforts of collective actors. And varied organizations using the same means may have different goals (e.g. public police in principle concerned with due process and justice as against private police concerned with protecting the interests of their employer).

In the case of the REPUVE, the distinction between private and public organizations is particularly relevant. A private organization, such as a car producer, possesses a set of organizational interests revolving around profit that are generally distinct from a public organization, such as a federal agency or state government bureaucracy, whose interests revolve around the execution of laws, policies, and bureaucratic procedures. On this basis, it would be reasonable to assume that a public organization would be more likely to support a surveillance program or the application of a technology for a public, security purpose, such as the REPUVE, than would a private organization, whose financial interests could be burdened by the costs of compliance. But such a reasonable expectation is betrayed by real world practice.

In Mexico, the greatest challenge to the REPUVE has come from the states, which by and large refused to implement the program. Speaking to program administrators within the SESNSP, the reasons for these difficulties were clear. They involved "resources" and "the will to get things done".

A public organization's implementation of a program such as the REPUVE requires a clear investment in resources. These include, at a bare minimum, computers to process information, printers to print out tags, hand-held RFID readers in order to activate and verify chips once they are adhered, and facilities and salaries for workers in the program. Some of the resources required by Mexican states to implement the REPUVE could be covered by the federal government, but the discrepancies between allocations and costs can be great. And without the funds on hand to dedicate to the program, many states in Mexico refused to implement the REPUVE.

Frustration over resources speaks to, in turn, the will or leadership to get things done. One SESNSP administrator Guzik spoke with opined that "this project has a very large scope, but sadly it has not been seen as such in the upper spheres, not at the Presidential level, nor the Interior Secretary level, nor the Public Security Secretariat level. They haven't given the program the enthusiastic backing that it should have … There is this feeling, it hasn't been made to succeed."

Conversely, while private organizations like car companies and their representatives complained both publicly and privately about the costs of complying with the REPUVE law, they largely complied. Why? In a communication with a REPUVE compliance officer at the SESNSP, Guzik was told that "the private sector has always been very strict, above all the big companies, with relation to legal compliance with the federal and state governments. It's not easy for their legal teams to know about a law or regulation and not comply with it."

Car producers themselves, meanwhile, saw compliance as part of their corporate culture and identity that reflected their responsible civic participation. As one car producer noted, "Why do [we] comply with the REPUVE law? [Our company] basically has 100% compliance with the law, not only the REPUVE law, but with all the laws, economic, import, customs, etc. We are the most precise and maybe the most compliant in the entire industry." Another company, importing vehicles from Asia, explained, "the Asian philosophy is very precise, very dignified in the sense that if the law asks me to do this, I have to comply … there are companies that are more rebellious, that in a given moment would sue and not comply. But the Asian companies aren't like that."

Organizations then are a vital component to understanding the fates of social control programs and technology. And if organizational interests coincide with the goals and plans of a particular surveillance program, they can be expected to support the effort. But such interests can be complicated, regardless of whether the organizations are governmental or not. And nonalignment of organizational interests can threaten the work of social control.

3. Political constitutions and legal obligations

If the goals and interests of agents and organizations are central to understanding control outcomes, it is also important to pay attention to the political and legal settings in which these entities operate. This is obvious in many respects, as an agent or subject of control and what their obligations are, are defined by the law. In the case of Mexico's automobile registry, for instance, the REPUVE law clearly defines the SESNSP as the authority over the registry, the states and federal agencies as federated entities and federal authorities, and private companies as obligated subjects with reporting responsibilities to the federal REPUVE.

But the impact of the law can work in more subtle ways as well. For instance, the reluctance of public organizations such as the customs offices and states to participate in the REPUVE is provided for under the Mexican constitution. Within Mexico's federalist political system, a reflection of the country's long history of dividing political power among regional strongmen, federal law does not apply to state governments the way that it does private corporations or individuals. As administrators with REPUVE complained, "the problem that we are having these days is that the private industry, the producers, 100% are participating. But the law requires them to … the states are autonomous. Free and sovereign. We cannot sanction them. We have to convince them. That's the challenge for us." Thus, Mexico's federal political constitution supports the expression and pursuit of different organizational interests.

But even for private organizations complying under the threat of punishment, the balance of power between political branches enshrined in Mexico's constitution provides a space for them to pursue their interests outside of the program. So it was that the Automotive Industry (AMIA) launched a lawsuit to reform the REPUVE law so that the states would have to register all vehicles. So, even though there was an agreement between the auto industry and the REPUVE, the industry did not stop in its efforts to alter the Public Registry of Vehicles Law so that its obligation would be done away with.

In these ways, legal contexts are central to outcomes. And we might expect more open political systems to offer more opportunities for actors and organizations to pursue their own interests or not comply. Similarly, federated political systems, such as in the US and Mexico, may differ from unitary republics, such as in France, where states and regions possess less autonomy from federal authorities. Autocratic political systems, meanwhile, would provide less opportunity to deviate from programs and federal, centralized plans.

4. Subjects and resistance

These considerations bring us to the topic of resistance. Marx (2016) has identified twelve general techniques of neutralization that subjects undertake to counteract surveillance. These are: (1) *discovery*, finding out whether surveillance is in operation; (2) *avoidance*, of the contexts or places that one knows will be subject to monitoring; (3) *piggy-backing*, where subjects directly face surveillance rather than avoid it, but evade control by attaching to a legitimate subject or object; (4) *switching*, when a subject transfers an authentic result to someone or something to which it does not apply; (5) *distorting*, moves to manipulate the surveillance-collection process such that, while test or inspection results are technically valid, the inferences drawn from them about performance, behavior, or attributes are invalid; (6) *blocking* and (7) *masking*, where the former makes inaccessible what is of interest to agents and the latter renders what is of interest unusable; (8) *breaking*, to render the surveillance device inoperable; (9) *refusing*, by subjects to cooperate under the terms desired by agents; (10) *explaining*, to account for an unfavorable result by explaining in order to cast doubt upon a tactic; (11) *cooperating*, where surveillance efforts can be neutralized or undermined if agents come to cooperate or collude with subjects; and (12) *counter-surveillance*, when subjects use the same tools as agents, and they may do so to record the behavior of agents.

Illustrations of these diverse tactics can be seen in drug testing. There, we see "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).

These strategies are present in and instructive for interpreting the outcomes of the REPUVE. In the states where the program was actually being implemented, subjects – drivers who are obligated to register their vehicles with the program – often refused. In other words, only a small number of drivers chose to provide themselves with the chance to harden their valuable targets from the threat of theft. And such a neutralization tactic threatened the viability of the program for those states looking to embrace it. State agents in those states were then left with having to brainstorm ways to lure drivers into the program.

5. Culture and stores of skepticism

If the lack of participation by drivers reflects strategic choices to not participate, it's also important to consider where such motivations derive from. Here, cultural factors specific to particular groups, regions, and countries can be seen to influence subjects' view of surveillance and social control.

In Mexico, for instance, federal car registries have a notorious history. Prior to the REPUVE, the Mexican government launched the National Registry of Vehicles (RENAVE). The RENAVE, like the REPUVE, was to include a database of vehicles manufactured, assembled, imported, or circulating in national territory in order to prevent contraband and automobile thefts. Unlike the REPUVE however, the program carried a registration fee (375 pesos, or $47, for new cars) and was operated by a private firm, Talsud. The RENAVE fell into disrepute when the head of Talsud, Ricardo Miguel Cavallo, was arrested in Cancún after it was learned that he was actually Miguel Angel Cavallo, an Argentine war criminal wanted by Spanish authorities for torture and other crimes committed during Argentina's military dictatorship in the late 1970s.

For drivers in Mexico, such stories remained present in their popular imagination and served as a ready well of mistrust when they encountered the REPUVE. As a technician with REPUVE explained, "There is 20% of the people that simply are not going to come, they're not going to come [to register]. Maybe they have bad information. They think that this is insecure, that we work for criminals, like RENAVE. RENAVE was a bad program that is distorting the REPUVE, because people think that it's the same story". Thus, the power of culture can impact seemingly unambiguous hard-engineered control efforts.

6. Technical tools and material objects of surveillance

Thus far, this review of the obstacles that can complicate social control activities through technology has been human-centric, focusing on the human actors and organizations that are central to control activities. Of course technology itself can be very important as well. Mirroring the distinction between the agents and subjects of social control, technology is central as a tool of control and as an object of control. And in both cases, technology can impinge upon the best laid plans of crime fighters.

In the case of tools, an obvious concern is whether a particular instrument is appropriate to the application it was chosen for. For the REPUVE, a controversy concerned passive versus active RFID technology. Following the REPUVE's launch, media reports cited experts who argued that the passive tags chosen by the SNSP had disadvantages such as poor read coverage and a high cost of reading equipment. Ultimately, the head of the SESNSP, Roberto Campa

Cifrián, was called to testify before Mexico's House of Deputies, the country's lower legislative chamber, to explain his decision on the bid. Earlier, he had said that the decision was made based on recommendations of an evaluation team from three of Mexico's universities and that their decision was informed by a consideration of chip lifespan, the lower costs per unit for passive chips, and the fact that passive technology was open source and not subject to proprietary restrictions. Unconvinced by the executive secretary's explanation, the House forced Campa Cifrián's resignation.

It is also important to consider the objects of surveillance, in this case automobiles. Even if subjects – drivers – want to register and participate in the REPUVE, objects can pose problems. One example here concerns VINs (Vehicle Identification Numbers). While there is no single standard for assigning VINs, the practice of assigning vehicles a 17-digit number identifying the car's manufacturer and characteristics, including model year, was adopted in many parts of the world in the early 1980s. But in Mexico, the international norm was applied beginning in 1997. Thus, vehicles produced in Mexico before that time could present particular difficulties. As an administrator with REPUVE explained, "Nissans and Volkswagens from 95, 96, 97, as well as Chevys from 94. They can't be put into the Public Registry of Vehicles for now. The system doesn't allow the registration of their serial numbers because of a production problem in those vehicles. The REPUVE system detected duplicate serial numbers in those brands, which caused the service to be suspended."

Automobiles have also proven tough to monitor on account of their windshields. Many vehicles have metallic particles (in their windshields) that prevent readings from REPUVE's equipment. Program administrators estimated that around 3 percent of the 25 million vehicles in the country, around 750,000, have such windshields. These vehicles cannot then be included in the registry. Thus, the reading of REPUVE's RFID tags has been complicated by the materiality it is meant to control.

7. Geography and the challenges of space

The technologies of social control do not exhaust the list of non-human, material elements that can complicate monitoring. Geography, the material or human-built landscapes upon which the daily activities of life are carried out, can also influence things. For instance, in the case of the REPUVE, program administrators found it challenging to plan for and implement the program in rural settings, which are set apart from the technical grids of urban centers which support the information technologies of social control.

In Zacatecas, a state with an appreciable rural population spread out over a large geographic area, planning how to ensure vehicles in rural areas were registered in the program posed a particular challenge. One technician there explained, "we know that in Zacatecas there exists a half-million registered vehicles, but there aren't a half-million vehicles. There's more. Some aren't plated. Others have American plates … Where are these people? In the villages. Why? Because maybe they make only a trip or two to the city. In the towns, in the cities, it's a bit stricter, because there's more people watching. There are cameras. You can't get away with as much. But there are villages that are very small, that have 1 or 2 traffic cops at most. And then, it's your buddy, your neighbor, your brother, or your father who's stopping you. And then it's just 'get on your way' [and nothing happens]." In this sense, the close-knit socio-political formations that are characteristic of rural areas prevent the implementation of hard-engineered control on the ground.

To respond to these geographic challenges, program leaders in Zacatecas decided to employ mobile registration modules, housed in mobile trailers that could be moved around the state in order to complete registrations. But in electing for mobile units over stationary ones, the computer equipment that the team used had to be broadcast remotely via radiofrequency. And the team registering vehicles experienced service interruptions that delayed the transmission of data from the registration site to the secretary's database. An administrator in Zacatecas noted that "I would ask the system specialists when they installed the system why the signal gets cut off. They said that these things are out of our hands. Maybe the telephone company, who administers the internet connection, had an issue. Or maybe there was a problem of some sort. Someone hit a telephone pole. Or someone was digging and cut the fiber optic cables."

The uncertainty principle

The preceding list of obstacles are not unique to Mexico or the REPUVE. Marc Schuilenburg's (2015) study of marijuana eradication campaigns and efforts to police road transport crimes in the Netherlands identified *dissimilar organizational interests* between policing agencies and housing associations (in the case of marijuana eradication) and policing agencies and insurance companies (in the case of road transport policing) as impediments to these novel security strategies. In the same work, he also notes how the *disparate goals of control agents* work against shop bans – shop owners are often unwilling to the invest the time and money into training their employees to identify shoplifters, which is necessary for the ban plan to work. Bigo (2006) and Cole (Chapter 29, this volume) touch upon related elements. Criminal courts in general were not enthusiastic about the wider use of lie detector tests in their proceedings for fear that their mechanic mode of truth-telling would make the court's human-based methods obsolete. In this sense, the courts possessed *dissimilar organizational interests* from the policing agencies promoting the machines. But more than this, "truth machines", like the "green technologies" studied by Brisman and South (Chapter 18, this volume), possess inherent *technical limitations* that complicate their programs of social control. Every way of doing something is also a way of not doing something else, with attendant gains and costs. Machines of "objective truth", even in the case of DNA identification technology, require a decent share of subjective processing and interpretation, and the production and use of green technologies always requires some element of environmental harm.

Our list of obstacles is hardly exhaustive. The discussion offers a starting point for future work to build on. And the preceding points are not intended to suggest that social control technologies are doomed to total failure. The REPUVE exists and operates today in Mexico. The reason it does is related to the program administrators' ability to respond to and work with the varying challenges noted. In Sonora, for instance, national REPUVE directors worked with state officials to fashion the registry into a tolling solution to provide residents free passage on federal highways. At the border, administrators convinced customs offices to participate in the program by allowing them to charge for car inspections, in seeming violation of the REPUVE law itself.

Such improvisations have been described as the "self-organizing processes" of security work (Schuilenburg 2015) or as "statecraft" (Guzik 2016). And they are critical to consider, since such alternations help shape the outcome and meanings of social control. For instance, in Sonora, the REPUVE is valued nearly universally there as a means for establishing and respecting a right to free transit that was fought for and established in the Mexican Revolution rather than a measure against vehicle thefts. At border crossings, the REPUVE is viewed negatively as another scheme to squeeze tax revenues out of individuals importing their vehicles from abroad. In Zacatecas, the REPUVE is understood and approached more cautiously as another governmental program promising to provide security. So then, although the REPUVE is functioning to realize *target identification* and *target hardening* in some parts of Mexico (but not others!), how its technology operates and what it means to people emerge in time and practice as administrators responded to challenges that were often difficult to anticipate when the program began.

In considering obstacles and improvisations and spaces to maneuver, we see *an uncertainty principle* at work with technologies and social control that belies the seeming objectivity and fixity of such efforts and the effort to fully reach a cherished engineering goal "to get the humans out of the loop." The factors we note make it likely that the application of surveillance technologies will often bring surprises. The hopes of utopians and fears of dystopians are rarely on target. Contexts need to be considered, and discretion and interpretation remain dance partners. There is usually room for humans to respond in ways not anticipated, or at least desired by planners. As Brisman and South (this volume) suggest, our "faith in magic wands" needs to be held in check.

But saying that uncertainty is inherent to social control and technology is not the same as saying that such efforts are wholly unpredictable. While uncertainty is inherent to technology and social control, systematic study and analysis can improve understanding and application.

At least five of the most prominent sources of uncertainty challenging to the best laid plans can be noted:

1 *Uncertainties of functioning* – technical artifacts may fail to work, break, or require costly unanticipated inputs and revisions; as they say, "stuff happens."
2 *Uncertainties of intended function* – most technical artifacts are not limited to their specified function. Thus Don Ihde (2008) has talked about the "designer fallacy" and the "ambiguous multistable possibilities" of artifacts. An airplane can get you to your destination, but also be a weapon to destroy buildings.
3 *Uncertainties of consequence* – technologies may bite back. (Aspirin can make one feel better, but taking too many can kill.) Policy and practitioners need to be particularly alert to gradient effects and short and longer time periods. Surprise outcomes are more likely when we fail to analyze the assumptions that are often buried (hidden?) deep within the celebratory rhetoric of technology's boosters (Appendix B lists a number of such techno-fallacies).
4 *Uncertainties of context* – social actors (individual or organisational) use their technological/behavioural extensions in ways which are unpredictable and often "irrational." Contexts with varied goals and interests may collide and react differently to the same tool.
5 *Uncertainties of environment* – physical environments can also be unpredictable and overwhelm the tool, as with the case of a meteorite hitting earth, or a monumental earthquake. A technology may work just fine as with the Fukushima Daiichi nuclear plant, but speaking metaphorically, only until there is a perfect storm in the form of the earthquake.

An example of one insight that future research into the relationship between the uncertainty principle and complexity is considered next. At the micro-level, social operations involving technology might be expected to encounter the fewest obstacles, since the number of agents, tools, subjects, and objects to monitor or control is limited. Take, for instance, the application of an RFID tag as an access solution for a parking garage, a hard-engineered solution to *target identification*. Generally, a single human agent with the tools of an RFID tag and electronic gate suffice to manage the operation, while the building management and company providing the service comprise the organizational setting. The rules for surveillance are largely defined by management. And the subjects are limited to those who want to access the garage and the number of vehicles that can fit in it. Finally, the material landscape of the parking garage is man-made and thus conducive to the application of man-made technological networks.

As surveillance is scaled up to a meso-level, the number of obstacles increases. Let's say we scale up RFID tag access from a parking garage to a tolling solution for state highways. Now, the agents increase, from a single guard to a state police force and local police forces. The organizational context changes as well. Beyond building garage management, we now have a state highway agency, police forces, political powers to authorize the program, corporations looking to compete for such a contract, and perhaps civic organizations that may oppose such a program. The number of subjects and objects of surveillance increases as well, as do the geographic challenges.

Scaling up to the macro-level, let's apply RFID tags for security on a national level, like the REPUVE, and the number of obstacles increases still. Federal police forces and agencies are added to the agents. Organizations now include federal agencies and political parties. National federal law, and international agreements on closed and open borders shift the legal context, as do constitutional guarantees. The number of subjects increases as well, as do the objects to be monitored. And geographic variability is enhanced still, from dry desert landscapes to dense rainforests. So the kinds of technologies we have considered must be accepted by a multiplicity of organizations, agents, and subjects, and be functional across a variety of material environments. And with open source technology, the technology must operate across a variety of providers.

By this logic, we can predict that macro-level efforts to achieve social control will be more uncertain than local efforts. And for those concerned with fighting crime, the uncertainty principle offers grounds to favor local applications, other factors being equal.

Those who look optimistically to technology as the solution to control problems and those who question it too often talk past each other. Both can reflect techno-fallacies embedded, and often unrecognized, in our culture (see Appendix B, drawn from Marx 2016) which identifies 44 such beliefs which may be fallacious on empirical, logical or value grounds. Particularly relevant here are: *the fallacy of a passive, nonreactive environment; the fallacy of more – if some is good, more must be better*; *the fallacy that the facts speak for themselves; the fallacy of explicit agendas; the fallacy of the sure shot; the fallacy of the fail safe system; the fallacy of delegating decision-making authority to the machine; the fallacy of the free lunch; and the fallacy that technology will always remain the solution rather than become the problem.*

Whether critic or advocate, there is a need to be aware of complexity and value conflicts and the need for empirical reality-checks. Liberty and democracy are fragile and not self-sustaining. The message for the independent scholar is to avoid premature commitment to the camp of either the optimists or the pessimists. Usually, the best answer is "it isn't clear" or "it depends." And then to take it further and indicate what needs clarification and what it depends on.

Let us finish with a contemporary implication of Odysseus's encounter with the Sirens. With the uncertainty principle in mind, the tale of Odysseus and the Sirens is not only about the heroism of its protagonist, as Homer would have us believe, nor about the ways technology can increase inequality, as per Horkheimer and Adorno. It is also a story about rationally applying a mechanical solution to a problem. Odysseus's Siren problem could be easily solved by a handful of beeswax. But today, the siren songs offered by technology's cheerleaders are more challenging and perhaps harder to resist. Amidst a deepening sense of crisis, they tempt us with simple engineered solutions sometimes bordering on the illusional, if not also the delusional, with the implication that our challenges can be met as successfully and with as little effort as Odysseus's. At such times it is well to recall another Greek myth, that of Icarus whose hubris was his undermining, as his wax wings melted when he flew too close to the sun.

References

Bell, Wendell (1997) Foundations of Futures Studies: History, Purposes, and Knowledge, Volume 1. New Brunswick, NJ: Transaction Publishers.

Bigo, Didier (2006) Globalized (in)security: The field and the ban-opticon, in Naoki Sakai and John Solomon (eds) *Translation, Biopolitics, Colonial Differences*, 109–156. Hong Kong: Hong Kong University Press.

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

Ellul, Jacques (1964) *The Technological Society*. New York: Vintage Books.

Gibbs, Jack P. (1989) *Control: Sociology's Central Notion*. University of Illinois Press.

Grabosky, Peter N. (1996) Unintended consequences of crime prevention, in Ross Homel (ed.) *Crime Prevention Studies*, Volume 5, 25–56. Monsey, NY: Criminal Justice Press.

Guzik, Keith (2016) *Making Things Stick: Surveillance Technologies and Mexico's War on Crime*. Berkeley, CA: University of California Press.

Hilgartner, Stephen, Richard C. Bell, and Rory O'Connor (1982) *Nukespeak: Nuclear language, visions, and mindset*. San Francisco: Sierra Club Books.

Homer. *The Odyssey*, A.S. Kline (trans.), available at: http://www.poetryintranslation.com/PITBR/Greek/Odyssey12.htm#_Toc90268047.

Horkheimer, Max, and Theodor W. Adorno ([1944] 1972) *Dialectic of Enlightenment*. New York: Herder and Herder.

Ozy (2016) The surprising link between Mountain Gorillas and iPhones. Feb. 18, 2016. www.ozy.com/fast-forward/the-surprising-link-between-mountain-gorillas-and-iphones/64539.

Ihde, Don (2008) The designer fallacy and technological imagination, in P. Vermaas, P. Kroes, A. Light and S.A. Moore (eds) *Philosophy and Design: From Engineering to Architecture*, 51–59. New York: Springer.

IRSS (2014) *Handbook of Increasing Resillence in Surveillance Societies*. http://irissproject.eu/?page_id=610&utm_source=IRISS_June2014&utm_campaign=8a7a98fc5a-IRISS_PR_Surveillance_in_Europe_10_10_2014&utm_medium=email&utm_term=0_a05fc7983f-8a7a98fc5a-174015249 (accessed October 1, 2014).

Janowitz, Morris (1975) Sociological theory and social control, *American Journal of Sociology*, 81(1): 82–108.

Lyon, David (2009) *Identifying Citizens: ID Cards as Surveillance*. Malden, MA: Polity.

Mander, Jerry (1992) *In the Absence of the Sacred: The Failure of Technology and the Survival of the Indian Nations*. San Francisco: Sierra Club Books.

Marcuse, Herbert (2002) *One Dimensional Man*. New York: Routledge.

Marx, Gary T. (1987) Raising your hand just won't do, *Los Angeles Times*. April 1, 2016.

Marx, Gary T. (1995) The engineering of social control: The search for the silver bullet, in John Hagan and Ruth D. Peterson, (eds) *Crime and Inequality*, 225–246. Stanford, CA: Stanford University Press.

Marx, Gary T. (2016) *Windows into the Soul Surveillance and Society in an Age of High Technology*. Chicago: University of Chicago Press.

Marx, Karl (1947) *Capital, volume 1*. New York: International Publishers.

Marx, Karl (1956) *Economic and Philosophical Manuscripts of 1844*. Moscow: Foreign Languages Publishing House.

Morozov, Evgeny (2011) *The Net Delusion: The Dark Side of Internet Freedom*. New York: Public Affairs.

Mumford, Lewis (1934) *Technics and Civilization*. London: George Routledge & Sons Limited.

Postman, Neil (1992) *Technopology: The Surrender of Culture to Technology*. New York: Knopf.

Rosner, Lisa (2004) *The Technological Fix: How People Use Technology to Create and Solve Problems*. London: Routledge.

Rule, James B. (1978) *Insight and Social Betterment: A Preface to Applied Social Science*. Oxford: Oxford University Press.

Schroeder, Ralph (1995) Disenchantment and its discontents: Weberian perspectives on science and technology, *Sociological Review* 43(2): 227–250.

Schuilenburg, Marc (2015) *The Securitization of Society: Crime, Risk, and Social Order*. New York: New York University Press.

Scott, James C. (1998) *Seeing Like A State: How Certain Schemes to Improve the Human Condition Have Failed*. New Haven, CT: Yale University Press.

Tenner, Edward (1997) *Why Things Bite Back: Technology and the Revenge of Unintended Consequences*. New York: Vintage.

Thorwald, Jürgen (1965) *The Century of the Detective*. New York: Harcourt, Brace & World.

Tucker, Robert (ed.) (1987) *The Marx-Engels Reader*. New York: W.W. Norton and Company.

Weinberg, Alvin M. (1967) Can Technology replace social engineering? *American Behavioral Scientist*, 10(9): 7–10.

Weizenbaum, Joseph (1976) *Computing Power and Human Reason*. San Francisco, CA: W.H. Freeman.

Wiener, Norbert (1967) *The Human Use of Human Beings: Cybernetics and Society*. New York: Avon Books.

Winner, Langdon (1988) *The Whale and the Reactor: A Search for Limits in an Age of High Technology*. Chicago: University of Chicago Press.

Appendix A

*Raising Your Hand Just Won't Do**

TO: ALL EMPLOYEES
FROM: EMPLOYEE RELATIONS DEPARTMENT
SUBJECT: RESTROOM TRIP POLICY (RTP)

An internal audit of employee restroom time (ERT) has found that this company significantly exceeds the national ERT standard recommended by the President's Commission on Productivity and Waste. At the same time, some employees complained about being unfairly singled out for ERT monitoring. Technical Division (TD) has developed an accounting and control system that will solve both problems.

Effective 1 April, [April Fool's Day] a Restroom Trip Policy (RTP) is established.

A Restroom Trip Bank (RTB) will be created for each employee. On the first day of each month employees will receive a Restroom Trip Credit (RTC) of 40. The previous policy of unlimited trips is abolished.

Restroom access will be controlled by a computer-linked voice-print recognition system. Within the next two weeks, each employee must provide two voice prints (one normal, one under stress) to Personnel. To facilitate familiarity with the system, voice-print recognition stations will be operational but not restrictive during the month of April.

Should an employee's RTB balance reach zero, restroom doors will not unlock for his/her voice until the first working day of the following month.

Restroom stalls have been equipped with timed tissue-roll retraction and automatic flushing and door-opening capability. To help employees maximize their time, a simulated voice will announce elapsed ERT up to 3 minutes. A 30-second warning buzzer will then sound. At the end of the 30 seconds the roll of tissue will retract, the toilet will flush and the stall door will open. Employees may choose whether they wish to hear a male or a female "voice". A bilingual capability is being developed, but is not yet on-line.

To prevent unauthorized access (e.g., sneaking in behind someone with an RTB surplus, or use of a tape-recorded voice), video cameras in the corridor will record those seeking access to the restroom. However, consistent with the company's policy of respecting the privacy of its employees, cameras will not be operative within the restroom itself.

An additional advantage of the system is its capability for automatic urine analysis (AUA). This permits drug-testing without the demeaning presence of an observer and without risk of human error in switching samples. The restrooms and associated plumbing are the property of the company. Legal Services has advised that there are no privacy rights over voluntarily discarded garbage and other like materials.

In keeping with our concern for employee privacy, participation in AUA is strictly voluntary. But employees who choose to participate will be eligible for attractive prizes in recognition of their support for the company's policy of a drug-free workplace.

Management recognizes that from time to time employees may have a legitimate need to use the restroom. But employees must also recognize that their jobs depend on this company's staying competitive in a global economy. These conflicting interests should be weighed, but certainly not balanced. The company remains strongly committed to finding technical solutions to management problems. We continue to believe that machines are fairer and more reliable than managers. We also believe that our trusted employees will do the right thing when given no other choice.

**Marx 1987. Appeared on April Fool's day, but many readers thought it was real. Is it more real today than in 1987?*

Appendix B

Techno-Fallacies

The social scientist focused on the empirical, logical and moral aspects of claims about technology for social control often hears statements that sound wrong. These techno-fallacies can involve elements of substance as well as styles of mind and ways of reasoning. Sometimes these fallacies are frontal and direct; more often they are tacit – buried within seemingly commonsense, unremarkable assertions. It is important to approach the commonplace in a critical fashion – whether we initially agree or disagree with the ideas.

This approach to analyzing the rhetoric of technology advocacy and consequences follows in the broad tradition of Mumford (1934), Ellul (1964), Weinberg 1967, Winner (1988), Postman (1992),Tenner (1997), Scott (1998), Marcuse (2002) and Rosner (2004) and of the more focused work on topics such as computers, the environment, energy, and crime (e.g. Wiener 1967; Weizenbaum 1976; Morozov 2011; Mander 1992; Hilgartner, Bell, and O'Connor 1982; Marx 1995; Grabosky 1996).

Beliefs may be fallacious in different ways. Some are empirically false or illogical. With appropriate evidence and argument, persons of goodwill holding diverse political perspectives and values may be able to see how they are fallacious, or in need of qualification.

Fallacies may also involve normative statements about what matters and is desirable. These reflect disagreements about values and value priorities. To label a normative belief a fallacy more clearly reflects the point of view of the labeler. However, normative positions are often informed by empirical assumptions (e.g. favoring controls that are presumed to eliminate discretion because they are believed to be more effective). In sniffing out fallacies, one must identify and evaluate the intermingling of fact and value and the quality of the facts (Rule 1978; W. Bell 1997). At a very general level, people often agree on values (though they often dissent over prioritizing and implementing these). Disagreements also commonly occur over what evaluation measure(s) and specific tools for judgment are most appropriate and over how evidence is to be interpreted—both with respect to what it says empirically and to its meaning for a given value.

Marx (2016) identifies five basic categories for organizing techno-fallacies:

A. Fallacies of technological determinism and neutrality
B. Fallacies of scientific and technical perfection
C. Fallacies involving subjects of surveillance
D. Fallacies involving questionable legitimations
E. Fallacies of logical or empirical analysis

Information age techno-fallacies

A. Fallacies of technological determinism and neutrality

1. The fallacy of autonomous technology and emanative development and use
2. The fallacy of neutrality
3. The fallacy of quantification
4. The fallacy that the facts speak for themselves
5. The fallacy that technical developments must necessarily mean less privacy

B. Fallacies of scientific and technical perfection

6. The fallacy of the 100 percent fail-safe system
7. The fallacy of the sure shot
8. The fallacy of delegating decision-making authority to the machine
9. The fallacy that technical solutions are to be preferred
10. The fallacy of the free lunch or painless dentistry
11. The fallacy that the means should determine the ends
12. The fallacy that technology will always remain the solution rather than become the problem

C. Fallacies involving subjects of surveillance

13. The fallacy that individuals are best controlled through fear
14. The fallacy of a passive, nonreactive environment
15. The fallacy of implied consent and free choice
16. The fallacy that personal information is just another kind of property to be bought and sold
17. The fallacy that if critics question the means, they must necessarily be indifferent or opposed to the ends
18. The fallacy that only the guilty have to fear the development of intrusive technology (or if you have done nothing wrong, you have nothing to hide)

D. Fallacies of questionable legitimations

19. The fallacy of applying a war mentality to domestic surveillance
20. The fallacy of failing to value civil society
21. The fallacy of explicit agendas
22. The legalistic fallacy that just because you have a legal right to do something, it is the right thing to do
23. The fallacy of relativism or the least bad alternative
24. The fallacy of single-value primacy
25. The fallacy of lowest-common-denominator morality
26. The fallacy that the experts (or their creations) always know what is best
27. The fallacy of the velvet glove
28. The fallacy that if it is new, it is better
29. The fallacy of equivalence or failing to note what is new
30. The fallacy that because privacy rights are historically recent and extend to only a fraction of the world's population, they can't be very important
31. The fallacy of the legitimation via transference

E. Fallacies of logical or empirical analysis

32. The fallacy of acontextuality
33. The fallacy of assumed representativeness
34. The fallacy of reductionism
35. The fallacy of a bygone golden age of privacy
36. The fallacy that correlation must equal causality
37. The fallacy of the short run

38. The fallacy that greater expenditures and more powerful and faster technology will continually yield benefits in a linear fashion
39. The fallacy that if some information is good, more is better
40. The fallacy of meeting rather than creating consumer needs (demand vs. supply)
41. The fallacy of the double standard
42. The fallacy that because it is possible to successfully skate on thin ice, it is wise to do so
43. The fallacy of rearranging the decks chairs on the titanic instead of looking for icebergs
44. The fallacy of confusing data with knowledge and technique with wisdom