Technology and Social Control

Gary T Marx, Massachusetts Institute of Technology (MIT), Cambridge, MA, USA

© 2015 Elsevier Ltd. All rights reserved.

Abstract

One aspect of modernization is the use of science-based technology in rule enforcement. In the 'engineered society,' an ethos of rationalization is seen in the application of means to ends. The events of 11 September 2001, and the war on terror have brought increased attention to the question, but the increased use of technical means for control reflects continuity rather than disjuncture. Six social control strategies are discussed and illustrated: target removal, target devaluation, target insulation, offender incapacitation, offender exclusion, and identification of offenses and offenders. In complex settings in a democratic society, relying primarily on technology to control human behavior has clear social and ethical limitations.

The technology's narrowing of focus may come at a cost of failing to see larger systemic contexts, alternatives, and longer range consequences. The complexity and fluidity of human situations makes this a rich area for the study of trade-off, irony, and paradox. There are some parallels to iatrogenic medical practices in which one problem is cured, but at a cost of creating another. Technical efforts to ensure conformity may be hindered by conflicting goals, unintended consequences, displacement, lessened equity, complacency, neutralization, invalidity, escalation, system overload, a negative image of personal dignity and the danger of the means determining, or becoming ends.

Introduction

Since the last half of the twentieth century, there has been a significant expansion in the use of science and technology for purposes of social control. Control through technology is central to the working of modern society. The events of 11 September 2001, and the war on terror have brought increased attention to the issue, but reflect continuity rather than disjuncture. Consider the intensification of control seen in the United States such as the Patriot Act and other legislation, and the creation of the Department of Homeland Security; vastly augmented expenditures for research and development; the international spread of tools such as DNA analysis, RFID chips, drones, facial recognition systems, enhanced travel and border controls, data-based risk management and predictive tools; and the increased sharing of information and integration among public and private and local, national, and international agencies.

Many technologies developed for the military such as the Internet, satellites, and sensors have diffused to other institutions. Yet the use of tools to engineer behavior goes far beyond particular historical events and national security to everyday life – whether this involves work, consumption, health, recreation, school, or families and friends.

The engineering of social control is one of the defining characteristics of modern society. 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.

In some ways, contemporary social control can be seen to reflect the ethos of the highly regulated prison in which conformity is sought by designing ever more features of the environment, rather than relying on trusting the individual or facing the uncertainty of human will and choice. Are new threats, technologies, expectations, and ways of living resulting in a move toward our becoming a 'maximum security society'? The engineering of control (in both its hard and soft forms) is an important component of our contemporary *surveillance society*. Marx (1985, 1988, forthcoming) expands on these developments. On surveillance more broadly, see Lyon (2007), Ball et al. (2012) and Staples (2000), and on technologies of crime control see Manning (1992) and Leman-Langlois (2013).

A major strand of social control involves the enforcement of rules and standards. This article provides a classification framework for technology-based efforts to prevent or reduce the harm from, or attractiveness of, rule violations and, when that is not possible, to increase the likelihood of discovering and apprehending violators. Such enforcement activities are distinct from other aspects of social control such as the creation of norms, processes of adjudication and sanctioning, or the broad societal guidance and integration that was of concern to early theorists of industrialization and urbanization (Gibbs, 1989; Janowitz, 1975).

The engineering of rule enforcement involves material artifacts (architectural and product design, sensors and alarms, access controls, and software), and also is distinct from forms of social control such as the creation and manipulation of culture, socialization, the redistributive rewards and penalties of the welfare state, and other interpersonal influences that are designed to influence behavior.

Contemporary efforts build upon, but go far beyond, a medieval fortification ethos. Of course, the inventors and builders of the first locks, safes, moats, and walled castles and the developers of early biometric identification systems (e.g., the Italian criminologist Cesare Lombroso, 1835–1909) were engaged in the engineering of social control. What is new is the scale and relatively greater scientific precision, power, omnipresence, continual invention and experimentation, and rapid global diffusion. Technical means of control saturate modern society, colonizing, documenting, and in some ways restricting ever more areas of life.

International Encyclopedia of the Social & Behavioral Sciences, Second Edition, 2015, 117–124

The roots of contemporary social control lie in the development of large organizations and standardized control technologies (Beniger, 1986). They are one strand of broad processes of rationalization, professionalization, and specialization occurring with modernization (Weber, 1958; Rule, 1973; Foucault, 1977; Cohen, 1985; Laudon, 1986; Gandy, 1993; Zuboff, 1988; Lyon, 1994; Shenhav, 1999). The heterogeneity, scale, mobility, and anonymity of mass society and the pursuit of efficiency and effectiveness encourage reliance on external, impersonal, distance-mediated, and technical means and database memories that locate, identify, register, record, classify, and direct individuals.

The perception of catastrophic risks in an interdependent, global world relying on complex technologies drives the search for definitive technical solutions. Consider issues such as terrorism, crime, obesity, drug abuse, acquired immunodeficiency syndrome, border controls, and the need for economic competitiveness and unprecedented flows of persons, information, and goods across borders. Developments in electronics, computerization, artificial intelligence, cognitive science, biochemistry, architecture, materials science, and many other areas promise new control possibilities. Entrepreneurial efforts (whether by private sector actors such as the security industry or governments such as the United States) have helped spread the technologies at home and abroad.

This use of contemporary technology contrasts with traditional approaches in which environments were less likely to be designed with rule enforcement in mind. Nor was there much probing beneath personal informational borders *before* untoward incidents occurred. Current preventive and anticipatory responses contrast with earlier reactive forms of control in which enforcement agents tended to become involved only *after* violations occurred and in a specific rather than a categorical fashion.

The engineering emphasis may be on environmental conditions, control agents, or actual or potential offenders and victims (sometimes the categories overlap). Consistent with the classical deterrence ideas that Thomas Hobbes (1588–1679) emphasized, some strategic efforts aim to create self-control and rational calculation on the subject's part others, however, seek greater certainty through applying hard engineering means believed to make the violation impossible. Rather than attend to the consciousness or will of subjects, the emphasis through automation is on eliminating, or at least significantly inhibiting, their ability to violate rules. Engineered efforts also seek to limit the ability of social control agents to demonstrate incompetence, mistakes, corruption, or discrimination, as the machine is geared to get 'the human out of the loop.'

Software programs aimed at prevention and early intervention have proliferated. There are many actuarial assessment protocols that profile and assign predictive scores to places and persons with respect to their presumed threat, vulnerability, and risk (Ericson and Haggerty, 1997). This has resulted in the expansion of various kinds of watch lists for at-risk populations such as the mentally ill, sex offenders, and those believed to be at risk of becoming homicide offenders or victims.

Any effort to *influence* persons or events can be seen as a form of engineered social control using tools exerted by an *agent* on a *subject* (or a population of potential subjects) or on an object. Engineering is present whenever a strategy based on beliefs about means–ends relations is applied and need not involve material factors. Prayers as well as magical practices would thus be examples, although they are far from the direct science-based efforts of interest here that involve rule enforcement. Failing to take any action as part of a strategy to avoid seeing a situation escalate is also an example.

Closer to the topic of the present article, although also distinct, is the design of presumably failsafe products *automated* for safety, such as the 'dead man's switch' on a train or the protective shield on a table saw – mechanisms that are intended to transcend human will. Engineering is also present in the *nonautomated* situations designed to persuade or guide behavior (but with choice remaining), such as advertisements for a negative political campaign or to discourage smoking, a waiter reciting the kinds of beers offered by moving from the least to the most expensive (anticipating that the customer will be prone to opt for the most recently mentioned beer), manufacturers increasing the nicotine or sugar content of cigarettes and food, or providing uncomfortable seating in fast-food restaurants to encourage rapid turnover. Also related are strategic efforts that permit, or even facilitate, *rule violations* through deception or reverse engineering. Consider police undercover operations, or online frauds that spoof computer security or create situations that permit blackmail. While sharing strategic logic, the above efforts are distinct from rule enforcement efforts.

Six Strategies

This section considers six engineering (primarily machine- or material-based) efforts to eliminate or limit violations by control of the physical and social environment, rather than by mere appeals to doing the right thing (or at least what an agent desires). This is followed by discussion of some social and ethical implications of such efforts.

The six ways of controlling persons and/or environments emphasize protection/alteration of the victim or the object of the violation (such as a car). Such actions make it impossible or at least more difficult or less inviting for the potential offender to act; or should prevention fail, tactics are intended to increase the likelihood of identification and apprehension. Some engineering efforts involve traditional notions of target hardening, but the engineering of control may also involve the idea of suspect softening or weakening.

Strategy 1 (and sometimes 4 and 5 below) includes *primary* direct prevention efforts. These are designed to eliminate the offense, or increase the difficulty of carrying it out. With the primary engineering strategy it is not necessary to affect the will or calculation of the potential rule breaker. The subjective orientations of the actor (whether based on calculation, a content-filled socialization, or a contentless discipline) are simply ignored. The emphasis is on altering opportunity structures and capabilities rather than the person's conscious choices. The social engineering example of castration as a device to control sexuality (whether literally or, as currently

may be done, chemically) clearly contrasts with appeals to virtue to accomplish the same end.

But primary strategies are not always available and may not live up to their promise. Hence, one sees a series of *secondary* engineering strategies (2, 3, 5, and 6 below) where concern with the will of the violator can be a factor. The more traditional goal of deterrence may be pursued by affecting the calculations of potential violators through devaluing and insulating targets, increasing the costs of nonconformity, and increasing the likelihood that violations and violators will be discovered and that evidence can be traced. What cannot, literally, be prevented may nonetheless be deterred by eliminating the gain, altering the cost-benefit ratio, or enhancing the chances for identification and apprehension.

As in other areas of social intervention such as public health, contemporary approaches place strong emphasis on preventing and minimizing harm. Rather than relying on persuasion (which assumes situations in which individuals have a choice about whether to respect a rule or to behave in a way that an agent wants them to), the emphasis is on direct technological interventions to design problems away. Ideally, problems are anticipated and eliminated (1, below); or where that is not possible, the goal is to create deterrence by reducing the gain (2), making violation more difficult and more costly (3, 4, 5), or by increasing the likelihood of identification and apprehension (6).

Target or Facility Removal

The logic of prevention is clearest and most effective here. 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. Police stings that pass off a harmless white substance as cocaine or that substitute fake for real dynamite or provide inoperable weapons offer evidence of intent to commit a crime, but preclude harm resulting from it. Conversely, deception as disguise may work in the other direction: hiding the appearance of something valuable, as with painting gold ingots black.

Target Devaluation

Here, the goal is to reduce or eliminate the value of a potential target to anyone but authorized users. The target remains, but its uselessness makes it unattractive to predators. Examples include products that self-destruct, as with some car radios when stolen, or that leave clear proof of theft, as with exploding red dye packs that stain money taken in bank robberies. The broken tamper proof seal on food products is intended to deter those who would tamper, and serves as a warning. Another type of example is telephones, computers, automobiles, and even guns that require a unique, presumably nontransferable biometric means of identification (e.g., retinal, voice, or geometric hand pattern) before they can be used. Disposable access codes that can only be used once need not be protected. Encrypted messages can often be easily intercepted, but without the decryption code the data are useless. As an antiteenager congregating tool, some mall shops play classical music in front of their stores.

Target Insulation

With this ancient technique, the object of desire persists but is protected. Perimeter maintaining strategies such as fences, walls, moats, guards, and guard dogs can be distinguished from more specific protections surrounding an object such as safes, armor, chastity belts, and goods that are in locked cases or chained to immovable objects. Other examples involve the hiding or disguising of valuables or persons. Still other examples involve high security, such as in gated communities where access and egress is carefully controlled, or make use of networked sensors, alarms, internet video, and bulletproof barriers, such as in banks separating customers from tellers (a form in Europe controls both entry into and exit from a bank through an enclosed booth). The architectural development of 'skywalks' linking downtown private buildings creates 'sanitary zones' more subject to control than the potentially disorderly public streets below. Softer forms of border protection lie in the use of access codes based on pin numbers, passwords, and biometric measures. Schools and after school programs can be seen as 'safe houses' in which the young are protected from offenders (and not incidentally school officials can watch the contained children for appropriate behavior).

Offender Weakening or Incapacitation

This classic strategy seeks to render potential offenders harmless by disabling or weakening their will or ability to violate the norm in question, or, if the violation occurs, to escape. The means may act directly on the body by permanently altering it and making certain offenses impossible – cutting off the hands of thieves – or at least uninviting, as exemplified in the operant conditioning seen in the novel *A Clockwork Orange* (Burgess, 1962).

A negative association with a particular form of undesirable behavior may be created. After ingestion of a substance such as antabuse, an unpleasant physical reaction (gagging or vomiting) follows when alcohol is consumed. The morphine derivative trexan is used to detoxify methadone as a remedy for heroin addiction.

Drugs such as Depo-Provera may be used to reduce sex drive and birth control implants, as well as sterilization, are sometimes judicially mandated. Lowering serotonin levels and psychosurgery have been used to curb violence.

Passivity, disorientation, or the inability to flee may be created by sensory weapons. Various citizen protection devices that can be defensively used such as mace fit here, as do nonlethal crowd control devices such as electrical, chemical, strobe, and acoustical immobilizers that disorient, stop, restrain, or block individuals (e.g., Tasers, pepper spray, loud music, flash bang devices, beanbag shotguns, sticky foam released on a floor, straitjackets, and a cage dropped upon or a net fired upon those to be controlled). Spikes in the road may be used to stop vehicles and some cars can be remotely stopped.

Related efforts deal not with the body of the offender but with the instrumentalities involved in the offense. Examples include antidrunk driving interlock systems, which require passing a breathalyzer test attached to the automobile ignition system before a car will start; cell phone muzzling devices for automobiles that use global positioning system (GPS) sensors to prevent the phone from being used while the car is being driven; or mixing a bad smelling chemical into a product to prevent it from being inhaled for its hallucinatory effects. An antipaparazzi device identifies the presence of a digital camera and can then remotely disable it through projection of a light beam.

Note also efforts at redefining the meaning of offender behavior. Thus, treating drug addiction as a medical rather than a criminal problem is in one sense a 'crime' elimination program. In some countries such as the Netherlands, there are safe drug houses where registered heroin users are provided drugs under carefully controlled circumstances. This lessens their need to commit crime to obtain the drugs and also offers a safe environment where they are protected from victimization. A *de facto* policy of toleration and damage control can also be seen in the formal creation of (or winking at) adult entertainment zones ('red light districts'). This can mean greater citizen awareness of victimization risks and some self-policing by service providers.

Exclusion

Potential offenders have traditionally been kept away from targets or tempting environments by exile, prison, curfew, and place or activity exclusions (e.g., restricting the sale of alcohol and cigarettes for juveniles). A related form is the visible warning offered by a stigma such as the brand or clipped ear for offenders in medieval Europe, which encouraged others to stay away. Fear of being degraded and ostracized as a result of stigmatization might also serve as a source of deterrence. Electronic monitoring or location devices based on GPS are contemporary examples. In one form, an alarm goes off and a message is sent to authorities if an adjudicated person wearing a transmitter gets too close to a prohibited person (such as an abused spouse) or leaves (or enters) a restricted area.

Capital punishment is the ultimate form of exclusion. At the other extreme is prevention of birth. With the human genome project completed, neoeugenic modes of exclusion are likely to be entertained. For example, the belief (which ignores interactions with the environment and the socially crafted character of most rules) that DNA is linked to violence and other antisocial behavior could generate another ultimate form of exclusion – requiring a license indicating an 'acceptable' genetic pattern before a child is permitted to be born (*see* DNA, Eugenics). Perhaps a less fanciful example (for the present at least) would be requiring special programs of education and even surveillance for individuals carrying the identified genetic patterns presumed to be associated with the behavior of concern. And with DNA databases, convicted (or otherwise included) individuals, and even close family members can be monitored for future acts.

Offense/Offender/Target Identification

Where it is not actually possible to physically prevent the violation, or where it is too expensive to do so, it may be possible to at least know that it took place and perhaps who is responsible, and to locate where the suspects are and/or where contraband may be stashed (as with X-ray, metal, and chemical detectors).

The goal is to document the violation and identify the violator. A major goal of nineteenth-century forensic science was to develop reliable biometric measures of identity based on the analysis of fingerprints, facial measurements, and mug shots, and chemical properties (Thorwald, 1965). These have significantly expanded from involving a person's gait and voice to tracking their distinctive smell. One technique used by the former East Germany involved identifying individuals by their unique olfactory signature. Architectural designs emphasizing visibility as a deterrent fit here (Newman, 1972), as do video, audio, motion, and heat detection devices and access codes that are presumed to document who enters or leaves an area, or is using a resource such as a computer. Hand-activated personal alarm systems, luggage alarms that go off if a purse or suitcase is illegitimately moved or opened, gunshot detection and location devices, cameras to detect speeders and red light violations, and the electronic tagging of consumer items in stores or books in libraries are other examples.

Hidden identification marks left on paper by the manufacturer or by photocopying machines and identifiers, in material that can be used to make explosives, would be included here. The various 'see something, say something' campaigns, which are dependent on the ease and ubiquity of multipurpose cell phones and e-mail, are a related example. Citizens are encouraged to use hotlines or smartphone apps to report, for example, suspicious persons and objects, erratic highway drivers, drug dealing, poaching, and organizational malfeasance. The police in turn use mass communications media to help identify and locate wanted persons via amber alerts, posting warrant information on Websites and crime reenactments on television, and posing as friends on Facebook pages.

Enhancements to criminal history data systems involving new tools for crime mapping of hot spots and analysis (e.g., Computer Statistics (COMPSTAT)) have appeared and there is increased sharing of information within and between control agencies and between the public and private sectors. There has been a significant expansion of surveillance practices for which there are no, or minimal, specific reporting requirements, as with GPS data, stored communication, and subscriber records (e.g., social media sites, texting, and Web browsing and searching).

Some Other Social Control Dimensions

The above categories are based on combining several aspects, such as whether the focus is on the potential offender, victim, or a resource that is part of the violation, and whether the means literally prevent or simply increase the risks and costs or decreases the attractiveness of violation. Combining separate dimensions into such ideal types can be useful as a shorthand way to classify and compare. Yet this approach can also distort

by merging sources of variation that can be analyzed separately and by excluding other variables.

Another approach starts with single dimensions that may cut across the different forms. Among relevant dimensions are classifications based on visibility or invisibility; openness or secrecy regarding use of the tactic both generally and specifically; control of access into or out of a system; emphasis on an individual, an organization, or a network; a focus on the body, consciousness, or the environment; reliance on machines, humans, or both; normative or nonnormative influences and, if the former, whether they involve criminal or civil law, policies, or manners; relative costs of a tactic including errors and mistakes; reliability and validity and ways of determining such costs; the presence or absence of democratic decision making, and review processes regarding the adoption and application of a tactic; and whether the goals of subjects and agents are the same, or at least overlap, or are in conflict. While all technological control efforts have elements in common, those involving dissensus and inequality are particularly important because of the centrality of human rights issues and the prominence of control and countercontrol efforts.

Some Social and Ethical Implications

Whether dealing with questions of justice, quality of life, security, health, the environment, or other issues, the potential benefits of science and technology are hardly deniable. In the case of criminal justice, for example, Clarke (1997) documents a number of successes. Yet given the sense of urgency about many problems and what is often the self-justifying tunnel rhetoric of those offering solutions, caution is needed, as well as midterm corrections, limitations, or prohibitions. To argue for a yellow light is certainly not a call to cease innovation or the search for better solutions.

However ideal a technical control system may appear in the abstract under ideal laboratory conditions, or however successful it may be in the short run, the world of application is often much messier and more complicated than the public relations efforts claim. There is rarely a perfect, or cost-free, technical fix (if nothing else, a given choice is likely to involve using resources that might have gone elsewhere). The technology's narrowing of focus on a given problem may come at the cost of failing to see larger systemic contexts, alternatives, and longer range consequences. The complexity and fluidity of human situations makes this a rich area for the study of trade-offs, irony, and paradox. Goal conflicts, unintended consequences, and sources of neutralization are among the factors limiting technical efforts to ensure conformity, as discussed below.

Goal Conflicts

At an abstract level, consider the possible tension between values. In the case of the new supermaximum security prisons, there is an enduring tension between the values of custody and punishment, as against care and some form of rehabilitation (Rhodes, 2004). More intensive mechanical control, whether within the prison or the community, often comes with a diminution of human contact and help with efforts to overcome the social and personal deficits that contribute to violations. Short-term gains in control may come at a cost of longer term losses (Byrne et al., 2007).

Informing subjects that a technique is in use is intended to serve the goal of deterrence, but such information may in turn serve as a strategic support for clever rule breakers who will then seek ways around it.

The expectation that one should be judged as an individual and in context may conflict with the greater rationality and predictive success believed to be found in categorical responses based on aggregate data and models divorced from the richness of particular situations. An automatic process that eliminates the misuse of authority and appears to offer fair (as in universal treatment) can conflict with the need to respond to the uniqueness of particular contexts. The latter requires discretion to potentially override action by a machine unable to take account of the concrete variation of the situation.

More concretely, goal conflicts in immediate situations can be considered. Thus, barriers need to prevent uninvited parties from entering a private space, while enabling those within such a space to leave in case of emergency. For example, bars over windows designed to keep out thieves may also prevent occupants from escaping through the window in the event of a fire. Conversely, barriers intended to keep persons or animals contained within a facility may lead to their being unable to get out when there is a fire (e.g., in a prison or a horse stall).

In commercial settings where access to merchandise is important, attaching expensive clothes (e.g., leather jackets) to a rack with a locked cable reduces the likelihood that an item will be stolen, but it also complicates trying clothes on and impulse buying. Encryption of information offers security, but at a cost of increased expense, slowing down the time required for a transaction and the risk of losing the key.

Unintended Consequences

Situations involving unexpected and unwanted results offer a rich area for analysis (Merton, 1957; Sieber, 1982; Marx, 1981; Tenner, 1997). It may be difficult to limit the impact of a technology. Terms such as blowback, collateral damage, spillover, backfire, and overshooting the target capture this. Techniques that immobilize suspects may do the same for control agents (e.g., sound wave technology intended to cause suspects to lose control of their bowels and a slippery banana peel substance that makes it difficult to walk). Uncontrollable wind patterns may send tear gas to places where it is not directed (including, literally, blowback on users). Consider the fact that enhanced lighting and lines of visibility can help perpetrators identify victims or control agents, as well as the reverse. The roads used by the Roman legions venturing forth to conquer became equally available to other conquerors who later marched on Rome. President Nixon, in an effort to secretly tape others famously also taped himself, leading to his downfall. Conversely, a protective device can lock everyone out when the keys are lost. The removal of benches from public areas denies the homeless, as well as others, a place to sit.

Automatic processes can result in punishment without trial. For example, *The New York Times* (28 December 1989) reported that a thief in Mobile, Alabama, was killed in a trap set by a homeowner. The trap consisted of two hunting rifles placed in

separate locations. One pointed down a staircase. The rifle fired when the thief stepped on a wire rigged to the trigger. A neighbor called the police when he heard a shot fired and then entered himself. It is easy to imagine good Samaritan scenarios that end disastrously (e.g., a passerby who is shot by a home-made burglar alarm after seeing a fire and rushing in to help).

Second-order effects also may occur. For example, when initially used, barrier strips intended to stop fleeing cars almost instantly released the air in the tires, sometimes causing high-speed crashes. Persons publicly identified as sex offenders may face vigilante attacks. The death of 30 persons in a fire in the London King's Cross subway station was attributed to fumes from antigraffiti paint. Enhanced technical enforcement along the United States–Mexico border has led to a funnel effect in which immigrants seek to enter through more dangerous desert areas with an increase in mortality (Cornelius, 2001).

An intervention may interact with other conditions to produce an undesired outcome. Thus, pepper spray is intended as a nonlethal alternative, but may be fatal to those with severe asthma or other respiratory problems. Consider also the warnings to pacemaker users that electronic sensors are in operation in retail settings. Will a nonlethal antitheft device that delivers a 50 000-V shock be lethal to the driver of a stolen car with a weak heart?

Moreover, there may be longer term health consequences that are not immediately visible. Questions have been raised, for example, about the effect of repeated exposure to radiation from X-ray search machines, particularly for children, the pregnant, and agents with repeated exposure (as reported in *The New York Times*, 26 April 2012).

Displacement

Several forms of displacement can be noted involving place, time, type of offense, and offender (Reppetto, 1976; Norris et al., 1998). Issues of displacement are central to many control settings where there are conflicts of interest and where rule breakers who have some resources find ways to beat control efforts.

The commercialization of protection, such as with embedding a hidden transmitter in cars that permits it to be located by remote electronic activation or gated communities to keep out would-be thieves, may lead to greater victimization of others who are unable to afford such enhanced levels of security.

Derivative offences may appear. The discovery that a target has been rendered useless to an offender may increase violence, whether as a resource to gain the needed access, or out of frustration. For example, the appearance of 'carjacking' is related to more sophisticated antitheft devices on cars. The use of access codes to activate autos and appliances may mean that the crime of burglary is converted to robbery or kidnapping when thieves confront property owners and demand not only the property but also the code to make it work. A frustrated thief may respond to a self-destruct automobile radio by fire-bombing the car.

New secondary laws that criminalize the possession of artifacts or activities designed to thwart enforcement may develop. Consider laws prohibiting the production, distribution, and use of products intended to falsify drug tests or for the possession of a radar detector designed to thwart traffic enforcement. In such cases, the guilty face charges for the secondary offense of possession, even when they were not committing the primary offense.

Neutralization and Escalation

Whether out of self-interested rule breaking, principled rebellion, or human contrariness, individuals can be very creative in neutralizing systems of control. In a free market economy, new controls create incentives to develop means of neutralization. This may lead to a higher level of play without fundamentally altering the game. A dynamic struggle may escalate, for example, when police use body armor and offenders react by using more powerful weapons and wearing armor themselves.

The fact that locks open with keys and borders require access points means they are eternally vulnerable. Marx (forthcoming) identifies a number of *behavioral techniques of neutralization* – strategic moves through which subjects seek to subvert controls. Reverse engineering permits a *breaking* move. For example, not long after antitheft ignition protection systems appeared on automobiles, a device that permitted bypassing the lock became available. No special tool is needed to spray paint over the lens of a video camera. In a *distorting* move, the initial antidrunk driving car interlock systems can be beaten by saving air in a balloon or by having someone else blow into it to start the car. A variety of moves can be seen in efforts to defeat urine drug tests. These range from contaminating the sample by pouring bleach on one's hand to the *switching* move of using a catheter to insert drug free urine into the body. *Discovery* moves are illustrated by a driver's use of radar detectors to locate police radar. When systems cannot be defeated technically, such as with sophisticated encryption technology, then their human context may be compromised, whether through coercion, corruption, or deception. For example, a thief who was unable to break a manufacturer's sophisticated encryption code, nevertheless managed to embezzle millions of dollars through generating fake invoices. He did this by having an affair with the individual who had the decryption codes.

In many settings, subjects have some rights and are entitled to challenge specific technological control. One thus sees *explanatory* moves through which an unfavorable result is reframed in an acceptable way by offering alternative data and citing the claims of rival experts, or making claims about rights and procedural violations. An *empirically valid* result does not guarantee a *socially meaningful* result. Thus, a DNA match between material from a crime scene and a suspect cannot reveal if the death in question resulted from a homicide or self-defense. Even when there is no question that a homicide occurred, the sample might have been planted or the evidential chain of custody may have been compromised. A computer match between persons on welfare and those with bank accounts may reveal a person whose account exceeded the savings limit, but such data do not provide proof of *cheating* since funds may have been held in trust for a funeral – a contingency that is legally permitted, but not necessarily built into the computer program. Audio and video recordings may reflect what was done and said, but may not reveal why, or what a suspect intended. Seeing should not automatically mean believing. Thus, a suspect in an undercover scheme may

have been threatened or entrapped off-camera. Nor does a drug test, even if 'valid,' indicate the presence of drugs within a person's system, a necessary indication of a violation. Depending on the assessment used, if the standard is set low enough it is possible to have a 'false-positive' reading as a result of just being in a room where marijuana was smoked or the result may be as a result of medications or eating certain foods.

Some Additional Factors

The overselling of technical solutions may exaggerate the risks, engendering immobilizing fear and leading to an unduly suspicious and distrustful society as well as wasting resources. Alternatively, an unexamined faith in a tactic's supposedly failsafe nature can lead to complacency and a false sense of security in which individuals are lulled into not taking necessary precautions. Consider a Los Angeles case in which a man sentenced to house arrest and required to wear an electronic surveillance bracelet shot and killed his estranged wife. She had not reported his threats to police because she thought she was safe as long as he had the bracelet on.

The seemingly ever-greater ease and efficiency offered by technological means can conflict with traditional liberty-protecting ideas of reasonable suspicion, minimization, and impracticality. Of course, as a folk expression holds, "if you hang them all you will certainly get the guilty." Risk prediction technology, as in the case of profiling, may be statistically accurate across many cases, but inaccurate with respect to a given case (this is the issue of aggregate rationality vs. individual cases). Even if accurate in an individual case as a prediction of future behavior, it may conflict with the individual's expectation to be judged on the basis of actual behavior.

Improvements in the ability to identify rule breaking may vastly expand the pool of 'suspects' who are subject to social control. Control systems may become overloaded, which can lower morale among enforcers who feel overwhelmed or offer corruptible officials a resource (nonenforcement) to market. Since resources for acting on all the available information may not be at hand, authorities may face charges of discriminatory enforcement.

Even when adequate resources for full enforcement action are available, organizational effectiveness can be harmed. Automatic technical solutions developed without adequate appreciation of complexity and contingency run the risk of eliminating the discretion, negotiation, compromise, and informal understandings that are often central to the morale and effective working of organizations (Dalton, 1959; Goffman, 1961). By broadening the documented pool of violations and violators, authorities may feel compelled to take action in cases that they otherwise think should be ignored. The rigidity of the machine and limited possibilities for immediate innovation can be damaging. One strand of humor involves the automatic, unthinking, and repetitive quality of many mechanical devices (such as in the classic Charley Chaplin film *Modern Times*).

If technical solutions were somehow to be effective at eliminating all rule breaking (leaving aside the conflict between, and the ambiguity of and lack of consensus on, many rules), such systems would risk becoming unduly rigid. Much innovation is initially seen as deviance. Experimentation and risk taking require latitude and can be aided by anonymity and secrecy. A socially transparent, engineered society would be more orderly, but likely less creative or dynamic and less able to respond to changing conditions.

If order depended only on technical means of blocking infractions, rather than on legitimacy, how would people behave if such technical means failed (e.g., in the case of a power failure and a failure even of backup systems)? A social order based primarily on technical fixes is likely to be as fragile over time as one based primarily on overt repression.

Even if systems could somehow be made fool- and fail-proof, with ever more advanced technology, there is a danger of viewing humans as robots, rather than as creative beings capable of making choices about how to behave. The former image is inconsistent with belief in the dignity of the autonomous individual in a democratic society. Whatever a technology is capable of, the view of humans as volitional (and hence responsible for their behavior) and beliefs about the inviolability (absent clear justification) of the borders that protect private personal zones around the human body, mind, relationships, communications, physical space, and past history are central to ideas of respect for personhood. The tools we use to communicate say something about how we see human beings and what kind of a society we live in and seek to create. Symbolism matters. So do precedents.

With new and seemingly effective social control techniques it is important to ask, "where might this lead and what kind of a society is being created?" In the United States, a future radically at odds with the nation's higher ideals is not likely to come about through cataclysmic change, but gradually in a thousand little ways, each perhaps understandable (if often aided by fear or seduction). In totality, however, such small changes can create a very different world – a world arrived at through accretion under the radar, rather than through full public dialogue.

The search for stand-alone mechanical solutions also avoids the need to ask why some individuals and groups break rules, and it points away from examining the social conditions that may contribute to violations and to the possibility of changing those conditions, rather than only trying to change the individual. Technical solutions seek to bypass the need to create consensus in a community in which individuals act responsibly as a result of voluntary commitment to the rules, not because they have no choice or fear reprisals. This emphasis can further social neglect and subsequent problems, leading to calls for more intensive and extensive reliance on technology in a seemingly endless self-reenforcing spiral.

There is a magisterial, legitimacy-granting aura around both law and science (Ericson and Shearing, 1986). Technological controls, presumed to be science based, are justified as valid, objective, neutral, universal, consensual, and fair. Their legitimacy may be strengthened in free market societies where such tactics often can be used by citizens (e.g., video cameras to record police behavior or DNA analysis offered by criminal defendants) and internally by police managers for guarding the guards.

Yet tools are socially created and their results are socially interpreted and thus potentially disputable. They exist in dynamic interdependent systems where interests may conflict, inequalities are often present, and where full impacts may be difficult to envision. Critical inquiry and humility are as needed, as are innovation and experimentation. It is important to maintain, if not a doubtful attitude, at least a respectfully skeptical attitude toward claims for the new; at least until they are examined both empirically and morally.

Our age has two rather distinct fears of technology. One, a la George Orwell, is that it will work all too well, creating a manipulated, totalitarian society naively taking pride in how free it is. The other fear, reflective of Franz Kafka, is that it would not work well enough. This suggests a crazily complex, out-of-control, interdependent, opaque society steeped in technological errors and *Catch-22* absurdities.

A well-known, if often naïve, expression (given that individuals and groups do not start with equivalent resources) holds that where there is a will there is a way. This points to the role of human motivation in obtaining goals. However, in light of the control possibilities made available by science and technology, this slogan can be reversed to "where there is a way there is a will."

The myth of Frankenstein implies that one must be ever vigilant to be sure that one controls the technology rather than the reverse. As Jacques Ellul (1964) argues, there is a danger of self-amplifying technical means silently coming to determine the ends, or even to become ends in themselves divorced from a vision of, and the continual search for, the good society.

See also: Civil Rights; Control, Social; Crime, Sociology of; Deterrence Theory: Crime; Deterrence; Empirical Legal Studies; Eugenics, History of; Forensic Genetic Databases: Ethical and Social Dimensions; Genetics and Forensics; Human Sciences, History of; Law and Society: Development of the Field; Police: A Sociology of Knowledge Approach; Power in Society.

Bibliography

Ball, K., Haggerty, K., Lyon, D., 2012. Routledge Handbook of Surveillance Studies. Routledge, London.

Beniger, J., 1986. The Control Revolutions: The Technological and Economic Origins of the Information Society. Harvard University Press, Cambridge.

Burgess, A., 1962. A Clockwork Orange. W.W. Norton, New York.

Byrne, J., Marx, G.T., 2011. Technological innovations in crime prevention and policing: a review of the research on implementation and impact. Journal of Police Studies 20 (3), 17–38.

Byrne, J., Taxman, F., Hummer, D. (Eds.), 2007. The New Technology of Crime, Law, and Social Control. Criminal Justice Press, Monsey, NY.

Clarke, R. (Ed.), 1997. Situational Crime Prevention: Successful Case Studies. Harrow and Heston, New York.

Cohen, S., 1985. Visions of Social Control. Polity Press, Cambridge.

Cornelius, W., 2001. Death at the border: efficacy and unintended consequences of US immigration control policy. Population and Development Review 27 (4), 661–685.

Dalton, M., 1959. Men Who Manage. Wiley, New York.

Ellul, J., 1964. The Technological Society. Vintage Books, New York.

Ericson, R., Haggerty, K., 1997. Policing the Risk Society. University of Toronto Press, Toronto.

Ericson, R., Shearing, C., 1986. The scientification of police work. In: Bohme, G., Stehr, N. (Eds.), The Knowledge Society: The Growing Impact of Scientific Knowledge on Social Relations. Reidel, Dordrecht.

Foucault, M., 1977. Discipline and Punish: The Birth of the Prison. Vintage, New York.

Gandy, O., 1993. The Panoptic Sort: Towards a Political Economy of Information. Westview Press, Boulder, CO.

Gibbs, J., 1989. Control: Sociology's Central Notion. University of Illinois Press, Urbana.

Goffman, E., 1961. Asylums. Anchor Books, Garden City, NJ.

Janowitz, M., 1975. Sociological theory and social control. American Journal of Sociology 81, 82–108.

Laudon, K., 1986. The Dossier Society: Value Choices in the Design of National Information Systems. Columbia University Press, New York.

Leman-Langlois, S., 2013. Technocrime, Technology, Crime and Social Control. Routledge, London.

Lyon, D., 1994. The Electronic Eye. Cambridge Polity Press, Cambridge.

Lyon, D., 2007. Surveillance Studies: An Overview. Polity Press, Cambridge.

Manning, P., 1992. Information technology and the police. In: Tonry, M., Morris, N. (Eds.), Modern Policing. University of Chicago Press, Chicago.

Marx, G.T., 1981. Ironies of social control: authorities as contributors to deviance through escalation, nonenforcement and covert facilitation. Social Problems 28, 221–246.

Marx, G.T., 1985. The Surveillance Society. The Futurist. June, 21–26.

Marx, G.T., 1988. Undercover: Police Surveillance in America. University of California Press, Berkeley.

Marx, G.T., forthcoming. Windows into the Soul: Surveillance and Society in an Age of High Technology. University of Chicago Press, Chicago.

Merton, R., 1957. Social Theory and Social Structure. Free Press, Glencoe, IL.

Newman, O., 1972. Defensible Space. MacMillan, New York.

Norris, O., Moran, J., Armstrong, G., 1998. Surveillance, Closed Circuit Television and Social Control. Ashgate, Aldershot.

Reppetto, T.A., 1976. Crime prevention and the displacement phenomenon. Crime and Delinquency 22, 166–177.

Rhodes, L., 2004. Total Confinement Madness and Reason in the Maximum Security Prison. University of California Press, Berkeley.

Rule, J., 1973. Private Lives, Public Surveillance. Allen-Lane, London.

Shenhav, Y., 1999. Manufacturing Rationality: The Engineering Foundations of the Modern Managerial Revolution. Oxford University Press, New York.

Sieber, S., 1982. Fatal Remedies. Plenum Press, New York.

Staples, W., 2000. Everyday Surveillance: Vigilance and Visibility in Postmodern Life. Rowman & Littlefield, Lanham, MD.

Tenner, E., 1997. Why Things Bite Back: Technology and the Revenge of Unintended Consequences. Vintage Books, New York.

Thorwald, J., 1965. The Century of the Detective. Harcourt Brace & World, New York.

Weber, M., 1958. In: Gerth, H., Mills, C.W. (Eds.), From Max Weber: Essays in Sociology. Oxford University Press, New York.

Zuboff, S., 1988. In the Age of the Smart Machine. Basic Books, New York.