Surveillance Studies

Gary T Marx, Massachusetts Institute of Technology, Cambridge, MA, USA

Abstract

This article suggests some basic terms for surveillance analysis. The analysis requires a map and a common language to explain and evaluate its fundamental properties, contexts, and behaviors. Surveillance is neither good nor bad but context and comportment make it so. Topics considered in this article include: a broad definition of surveillance, its strategic and nonstrategic forms, and the traditional and new surveillance. A family of related terms – privacy, publicity, confidentiality, and secrecy – is also considered. The discussion next focuses on characteristics of the social structures that organize behavior, the characteristics of the *means* used, and some value conflicts and social processes seen with the emergent, interactive character of much surveillance behavior.

Queen Elizabeth (1533–1603) introduced modern ideas about the rights of the person including protection against "windows into men's hearts and secret thoughts." In this view, she draws on an English proverb: "the eyes are the windows into the soul" that in turn reflects the biblical claim (Matthew 6: 22–23) that probative looking into another's eyes reveals who they are (questions of deception and validity apart). Queen Elizabeth realized that the dignity of the person requires limits on looking, particularly when coercion and inequality are present, as with state power. Yet as a ruler concerned with the welfare of her subjects she needed information about them, as well as about rule breakers and those who would overthrow her government. Her challenge – juggling the protection of individuals' hearts and secret thoughts and the protection of state security – is one that faces democratic leaders everywhere.

This article suggests some basic terms for surveillance analysis. A map and a common language are required to explain and evaluate its fundamental properties, contexts, and behaviors. The empirical richness of watching and being watched (whether involving the eye or other senses and various kinds of data) and the uses of surveillance results need to be disentangled and parsed into basic categories and dimensions. After offering a brief comment on surveillance studies and a broad definition of surveillance, attention is given to strategic and nonstrategic forms, and traditional and the new forms of surveillance. A family of terms related to surveillance – privacy, publicity, confidentiality, and secrecy – is considered. The discussion next focuses on characteristics of the *social structures* that organize behavior and the characteristics of the *means* used and some *social processes* seen with the emergent, interactive character of much surveillance behavior. I next turn to value conflicts that make surveillance often so controversial. The discussion that follows draws from Marx (2015, and articles at www.garymarx.net) and is informed by the sources in **Table 1**.

What Is Surveillance?

Today's *surveillance society*, as is involves the state, the private sector, and interpersonal relations, brings forth the same paradox faced by Queen Elizabeth noted in the preceding paragraph – whether the National Security Agency's worldwide gathering of metadata on telecommunications, or merchants, employers, and parents watching customers, workers, and children, respectively. In a world where surveillance is seen as both a response to threats and a threat, before asking "Is surveillance good or bad?" we need to ask, "What concepts are needed to capture its basic structures and processes?" Surveillance as such is neither good nor bad, but context and comportment do make it so. The same can be said for the related concept

Table 1 Surveillance essays: names of the new society and its key aspects[a]

The panopticon (Bentham, 1995)
Disciplinary society, the gaze and bio-power (Foucault, 1977, 1998)
Surveillance society, the new surveillance and maximum security society (Marx, 1985, 2015)
Net widening (Cohen, 1985)
Dossier society (Laudon, 1986)
Dataveillance (Clarke, 1988)
Super-panopticon (Poster, 1990)
Society of control (Deleuze, 1992)
L'anamorphose de l'etat-nation (Palidda, 1992)
Panoptic sort (Gandy, 1993)
Minimum security society (Blomberg, 1987)
Synopticon (Mathiesen, 1997)
Securitization (Buzan et al., 1998)
Telematic society (Bogard, 1996)
Techno-policing (Nogala, 1995)
Transparent society (Brin, 1998)
The maximum surveillance society (Norris and Armstrong, 1999)
Liquid modernity (Bauman, 2000)
Information empire (Hardt and Negri, 2001)
Surveillant assemblage (Haggerty and Ericson, 2006)
Post-panopticon (Boyne, 2000)
Glass cage (Gabriel, 2005)
Ban-opticon (Bigo, 2006)
High policing (Brodeur and Leman-Langlois, 2006)
Ubiquitous computing (Greenfield, 2006)
Ubereveillance (Michael et al., 2008)
Ambient intelligence (Wright et al., 2008)
Safe society (Lyon, 2007)
Thick and thin surveillance (Torpey, 2007)

[a]A representative, although hardly exhaustive, list.

International Encyclopedia of the Social & Behavioral Sciences, Second Edition, 2015, 733–741

of privacy. Context refers to the type of institution and organization in question and to the goals, rules, and expectations they are associated with. *Comportment* refers to the kind of behavior expected (whether based on law or less formal cultural expectations) of, and actually shown by, those in various surveillance roles.

While sharing some elements, differences in surveillance contexts involving coercion (government), care (parents and children), contracts (work and consumption) and free-floating accessible personal data (the personal and private within the public) need consideration. Surveillance is a generic process characteristic of living systems with information borders and not something restricted to governments, spying, or secrecy. Surveillance and privacy are not necessarily in opposition and the latter can be a means of insuring the former as with access controls to information. While media attention to the problems associated with inappropriate surveillance (particularly by government) is present, there are also problems associated with the failure to use surveillance when it is appropriate. The emerging interdisciplinary field of surveillance studies analyzes these issues.

Surveillance Studies

The watchful and potentially wrathful (although also sometimes loving and protective) eye of the Biblical God of the Old Testament offers an early example of surveillance. More modern authors include Hobbes, Rousseau, Bentham, Marx, Nietzsche, Weber, and Taylor. Foucault (1977) (although writing about earlier centuries) is the grandfather of contemporary surveillance studies.

The field of surveillance studies came to increased public and academic attention after the events of 9/11 (Monaghan, 2006; Ball et al., 2012). But the topic in its modern form has been of interest to scholars at least since the 1950s. This is related to greater awareness of the human rights abuses of colonialism, fascism, and communism and anti-democratic behavior within democratic societies. The literary work of Huxley, Orwell, and Kafka and the appearance of computers and other new technologies with their profound implications for social behavior, organization, and society are also factors in the field's development.

In the form of *the surveillance essay* current writers from many disciplines and perspectives (e.g., political economy, social control, law and society, and criminology) draw on and extend the earlier theorists to describe the appearance of a new kind of society with new forms of social ordering (Table 1).

As ideal types, the terms in Table 1 such as the 'panopticon,' 'disciplinary society,' or 'maximum security society' combine many strands that need to be separated if we are to move beyond sweeping claims made about surveillance. The concepts discussed in this article seek to bring greater precision and to add some leaves to the trees. One way to do that is to develop a middle range approach that fills out a general concept such as the *maximum security society* (as well as most of the other broad surveillance society naming concepts in Table 1) by identifying subsocieties that compose the surveillance society.

The maximum society concept draws parallels to the *total institution* and the maximum security prison and suggests that forms of control traditionally associated with the prison are diffusing into the broader society. But as an abstract notion, it does little to analyze variation in surveillance practices and changes over time. To do that the threads of the tapestry must be unwound in a series of subsocieties. Among components of the contemporary surveillance society are: a *hard engineered society*; a *soft and seductive engineered society*; a *dossier society*; an *actuarial society*; a *transparent society*; a *self-monitored society*; a *suspicious society*; a *networked society* of ambient and ubiquitous sensors in constant communication; a *safe and secure society* with attenuated tolerance for risk and with a strong emphasis on prevention; a '*who are you society?*' of protean identities, both asserted by and imposed upon individuals; and a '*where are you, where have you been, and who else is there?*' *society* of documented mobility, activity, and location. The broad approach of the surveillance essays is important in calling attention to contemporary changes, but such work generally does not take us beyond broad statements, does not adequately define surveillance, nor identify components that would systematically permit differentiating the new from the old forms, or making comparisons between various surveillance uses, contexts, and societies. In offering neither inclusive and nuanced definitions nor adequately elaborating dimensions, they fail to call attention to what is universal in human societies or to offer ways to analyze what is different.

Defining Surveillance

The English noun *surveillance* comes from the French verb *surveillir*. It is related to the Latin term *vigilare* with its hint that something vaguely sinister or threatening lurks beyond the watchtower and town walls. Still, the threat might be successfully warded off by the vigilant. This ancient meaning is reflected in the association many persons still make of surveillance with the activities of police and national security agencies. Yet in contemporary society the term has a far wider meaning.

What is surveillance? The dictionary, thesaurus, and popular usage suggest a set of related activities: look, observe, watch, supervise, control, gaze, stare, view, scrutinize, examine, checkout, scan, screen, inspect, survey, glean, scope, monitor, track, follow, spy, eavesdrop, test, or guard. While some of these are more inclusive than others and can be logically linked (e.g., moving from look to monitor), and while we might tease out subtle and distinctive meanings for each involving a particular sense, activity, or function, they all reflect what the philosopher Ludwig Wittgenstein calls a family of meanings within the broader concept.

At the most general level surveillance of humans (which is often, but need not be synonymous with human surveillance) can be defined as regard or attendance to others (whether a person, a group, or an aggregate as with a national census) or to factors presumed to be associated with these. A central feature is gathering some form of data connectable to individuals (whether as uniquely identified or as a member of a category).

A verb such as 'observe' is not included in the definition because the nature of the means (or the senses involved) suggests subtypes and issues for analysis and ought not to be foreclosed by a definition (e.g., how do visual, auditory, text, and other forms of surveillance compare with respect to factors such as intrusiveness or validity?). If such a verb is needed, to 'scrutinize,' 'regard,' or 'attend to' is preferable to observe, with its tilt toward the visual.

Many contemporary theorists offer a narrower definition tied to the goal of control (e.g., Dandeker, 1990; Lyon, 2001; Manning, 2008; Monahan, 2010). Taking a cue from Foucault's earlier writings, control as domination is emphasized (whether explicitly or implicitly) rather than as a more positive direction or neutral discipline. Yet, as Lianos (2003) observes, the modern role of surveillance as control must be placed in perspective alongside its fundamental importance in enhancing institutional efficiency and services.

Surveillance – particularly as it involves the state and organizations, but also in role relationships as in the family – commonly involves power differences and on balance favors the more powerful. Understanding this is furthered with comparisons to settings where control and domination are not central as with other goals such as surveillance for protection, entertainment, or contractual relations; where surveillance is reciprocal; and where it does not only, or necessarily, flow downward or serves to disadvantage the subject.

Authority and power relations are closely related to the ability to collect and use data. The conditions for accessing and using information are elements of a democratic society (Haggerty and Samatas, 2010). The greater the equality in subject–agent settings, the more likely it is that surveillance will be bilateral. Given the nature of social interaction and a resource-rich society with civil liberties, there is appreciable data collection from below as well as from above and also across settings. Reciprocal surveillance can also be seen in many hierarchal settings.Mann et al. (2003) refer to watchful vigilance from below as *sousveillance*.

The definition of surveillance as hierarchical watching over or social control is inadequate. The broader definition offered here is based on the generic activity of surveilling (the taking in of data). It does not build in the goal of control, nor specify directionality. In considering current forms we need to appreciate bidirectionality and horizontal as well as vertical directions. Control needs to be viewed as only one of many possible goals and/or outcomes of surveillance. When this is acknowledged, we are in a position to analyze variation and note factors that may cut across kinds of surveillance.

In his analysis of "The Look" Sartre (1993) captures a distinction between *nonstrategic* and *strategic surveillance*. He describes a situation in which an observer is listening from behind a closed door while peeking through a keyhole when "all of a sudden I hear footsteps in the hall." He becomes aware that he himself will now be observed. In both cases he is involved in acts of surveillance, but these are very different forms. In the latter case he simply responds and draws a conclusion from a state of awareness. In the former he has taken the initiative, actively and purposively using his senses.

Nonstrategic surveillance refers to the routine, autopilot, semiconscious, often even instinctual awareness in which our sense receptors are at the ready, constantly receiving inputs from whatever is in perceptual range. Smelling smoke or hearing a noise that might or might not be a car's backfire are examples. In contrast, strategic surveillance involves a conscious strategy to gather information. This may be in a cooperative or adversarial setting – contrast parents watching a toddler with corporations intercepting each other's telecommunications.

Within the strategic form, which to varying degrees ferrets out what is not freely offered, we can identify two mechanisms intended to create (or prohibit) conditions of visibility and legibility: material *tools* that enhance (or block) the senses and *rules* about the surveillance itself. While these are independent of each other, they show common linkages, as with rules requiring reporting when there are no available tools for discovery or rules about the conditions of use for tools that are available. A stellar example is the 'Lantern Laws' that prohibited slaves from being out at night unless they carried a lantern (Browne, 2015). Here, the emphasis is on requiring the subject to make him or herself visible given the limitations brought by darkness. But note also efforts to alter environments to make them more visible as with the creation of 'defensible space': via taking down shrubs or using glass walls (Newman, 1972) or less visible ala the architecture of bathrooms.

Within the strategic form we can distinguish traditional from the new surveillance. Examples of the new surveillance include computer matching and profiling, big data sets, video cameras, DNA analysis, GPS, electronic work monitoring, drug testing, and the monitoring made possible by social media and cell phones. The new surveillance tends to be more intensive, is extensive, extends the senses, is based on aggregates and big data, has lower visibility, involves involuntary (often categorical) compliance of which the subject may be unaware, tends to decrease cost, and reach remote locations. While the historical trend here is clear, it is more difficult to generalize about other characteristics such as whether or not surveillance has become more deceptive or more difficult to defeat than previously. Many forms are more omnipresent and often presumed to be omnipotent.

The new surveillance may be defined as scrutiny of individuals, groups, and contexts through the use of technical means to extract or create information. In this definition the use of 'technical means' to extract and create the information implies the ability to go beyond what is naturally offered to the senses and minds unsupported by technology, or what is voluntarily reported. Many of the examples extend the senses and cognitive abilities by using material artifacts, software, and automated processes, but the technical means for rooting out can also involve sophisticated forms of manipulation, seduction, coercion, deception, infiltrators, informers, and special observational skills.

Including 'extract and create' in the definition calls attention to the new surveillance's interest in overcoming the strategic or logistical borders that inhibit access to personal information. These inhibitors may involve willful hiding and deception on the part of subjects or limits of the natural world, senses, and cognitive powers. Create also suggests that data reflect the output of a measurement tool. The tool itself reflects a decision about what to focus on and the results are an artifact of the way they were constructed. Of course, constructions vary in their usefulness, validity, and reliability. Our perceptions of the empirical world are conditioned by where and how we look and these may vary in their fidelity to that world.

The use of 'contexts' along with 'individuals' recognizes that much modern surveillance attends to settings, or patterns of relationships and groups, beyond focusing on a given, previously identified individual. Meaning may reside in cross-classifying discrete sources of data (as with computer matching and profiling) that, when considered separately, are not revealing. Systems as well as persons are of interest. The collection of group data or the aggregation of individual into group data offers parameters against which inferences about individuals are drawn for purposes of classification, prediction, and response. Depending on the parameters, this may bring rationality and efficiency, but there is an inferential leap in going from *group* characteristics based on *past events* to *future* predictions about a given *individual*.

This definition of the new surveillance excludes the routine, nontechnological surveillance that is a part of everyday life, such as looking before crossing the street or seeking the source of a sudden noise or an unusual scent. It also excludes the routine attentiveness to, and interaction with, others that is fundamental to being a social being (as with mannerly behavior such as opening the door for another or offering a seat to an elderly person). An observer on a nude beach or police interrogating a cooperative suspect would also be excluded, because in these cases the information is volunteered and the unaided senses are sufficient.

Related but Distinct: Surveillance and Privacy, Privacy, and Publicity

How do surveillance and privacy relate? Surveillance is often wrongly seen to be the opposite of privacy. Kelvin (1973) emphasized this role of privacy as a nullification mechanism for surveillance. But at the most basic level, surveillance is simply a way of discovering and noting data that may be converted to information. Thus, depending on the context and role played, individuals or groups may be required, find it optional, or be prohibited from engaging in these activities, whether as subjects or agents of surveillance and communication. This obviously can involve invasions of privacy, as it was with the employee in a lab testing for AIDS who sold information on positive results to a mortuary.

Yet surveillance can also be the means of protecting privacy. Consider biometric identification and audit trails required to use some databases, or defensive measures such as a home security video camera. Privacy for whom, surveillance of whom, by whom, and for what reasons need to be specified.

Privacy like *surveillance* is a multidimensional concept whose contours are often ill-defined, contested, negotiated, and fluid, dependent on the context and culture. Among the major forms are *informational* (Westin, 1967), *aesthetic* (Rule et al., 1980), *decisional* (Decew, 1997), and *proprietary* (Allen, 2007) privacy. Informational privacy (Westin, 1967) is the most significant and contested contemporary form and involves the rules and conditions around personal information.

Breaches of decisional or proprietary privacy involve application or use of private information, rather than information discovery. While distinct, informational privacy shares with the other forms the key factor of control over access to the person or at least the person's data and the forms may be temporally connected. Thus, if individuals can control their personal information – whether not having to reveal their purchase of birth control pills (when this was illegal) or keeping paparazzi from taking pictures – they need not worry about that information being used.

Informational privacy encompasses *physical privacy*. The latter can refer to insulation resulting from natural conditions such as walls, darkness, distance, skin, clothes, and facial expression. These can block or limit outputs and inputs. Bodily privacy is one form of this, and its borders can be crossed by implanting something such as a chip or birth control device or removing something, such as tissue, fluid, or a bullet. Within informational privacy we find the conditions of anonymity and pseudo-anonymity, often referred to as being necessary for another type of privacy involving seclusion and being left alone. Personal information borders are obviously more difficult to cross if an individual cannot be reached via name or location.

Informational privacy can be considered as it ties to institutional setting (e.g., financial, educational, health, welfare, employment, criminal justice, national security, voting, and census); places and times; the kind of data involved, such as about religion or health; participant roles; and aspects of technology and media, such as audio or visual, wire or wireless, print, phone, computer, radio, or TV. Considerations of setting, location, time, data type, and means are central to legislation and regulation and rich in anomalies and cross-cultural differences.

A concept related to privacy is publicity. The two can be linked within the same framework. The common elements are rules about the protection and revelation of information. In some countries such as Canada the same officials are responsible for privacy and for freedom of information. In the first case there are rules giving individuals the right to control their personal information and in the second rules requiring that information not be restricted – that is, that it be made public. While sharing elements, for policy purposes there are major differences between the privacy of individuals and the secrecy of organizations. The standards for the latter should not automatically be applied to the former.

As nouns privacy and publicity can be seen as polar ends of a continuum involving rules about withholding and disclosing, and seeking or not seeking, information. Thus, depending on the context and role played, individuals or groups may be required, find it optional, or be prohibited from engaging in these activities, whether as subjects or agents of surveillance and communication.

When the rules specify that a surveillance agent is not to ask certain questions of (or about) a person and the subject has discretion about what to reveal, we can speak of *privacy norms*. When the rules specify that the subject must reveal the information or the agent must seek it, we can speak of *publicity norms* (or, better perhaps, disclosure norms). With publicity norms there is no right to personal privacy that tells the agent not to seek information, nor does that give the subject discretion regarding revelation. Rather, the reverse – the subject has an obligation to reveal and/or the agent to discover (Marx, 2011).

The moral expectations surrounding information as a normative phenomenon (whether for protection as with

privacy or revelation as with publicity and whether based on law, policy, or custom) can be differentiated from the empirical status of the information as known or unknown. To understand this distinction, we need the related terms, private and public – adjectives that can tell us about the status of information. Is information known or unknown, does it have an objective quality, can it be relatively easily measured? For example, in face-to-face encounters one generally knows the gender and face of a stranger, whether this is in the street, an office, or a home. The information is 'public' as in readily accessible, and this may be supported by anti-mask laws and requirements to wear symbolic items of clothing, tattoos, or badges. Absent such rules, the stranger's political or religious beliefs are more likely to be invisible and unknown.

Normative expectations of privacy and publicity do not always correspond to how the adjectives public and private are applied to empirical facts. Thus, the cell phone conversations of politicians and celebrities that have privacy protections may become public. Information subjected to publicity requirements such as government and corporate reports and disclosure statements may be withheld, destroyed, or falsified. Information not entitled to privacy protections, such as child or spouse abuse, may be unknown because of the inaccessibility of the home to broader visibility. The distinction calls for empirical analysis of the variation in the fit between the rules about information and what actually happens to it.

Privacy and publicity can be thought of in literal and metaphorical spatial terms involving invisibility–visibility and inaccessibility–accessibility. The privacy offered by a closed door or a wall and an encrypted e-mail message share information restriction, even as they differ in many other ways. Internet forums are not geographically localized, but in their accessibility can be usefully thought of as public places, not unlike the traditional public square where exchanges with others are possible or where others are visible as with open architecture. Erving Goffman (1971) in writing of 'relations in public' and 'public life' attends to the elements and possibilities within the immediacy of physical copresence. This is the strand of 'publicness' as visibility. It suggests the 'public' as known to at least one other person rather than to any rules about the status of information (that it must be revealed or concealed or to a legally defined place such as private golf course) as noted above. Thus, we can paradoxically speak of 'public order in private places' (Goffman, 1971: XIV).We can also speak about expectations of the private even within the public (Nissenbaum, 1998; Marx, 2001). In the latter case, since the information is available (such as with someone's appearance or a conversation overheard in a restaurant). But limits remain as with expectations about not staring or listening too closely to what others nearby are saying.

Structures and Processes

Regardless of whether we are dealing with traditional or the new surveillance, some common classificatory notions can be applied. In the case of surveillance social structures, for example, we can identify the *surveillance agent* (whether as watcher/observer/seeker/inspector/auditor/tester), while the person about whom information is sought or reported is the *surveillance subject*. The agent role can be further separated into the *sponsor*, *data collector*, and *initial* or *secondary user*.

Many contemporary concerns over surveillance involve the practices of large organizations relative to employees, clients, or the public. *Organizational surveillance* is distinct from the *nonorganizational surveillance* carried about by individuals. At the organizational level, formal surveillance involves a constituency. Organizations have varying degrees of internal and external surveillance (Rule, 1973). Erving Goffman (1961) has identified many kinds of employee or inmate monitoring, such as within 'total institutions.'

Within an organization *internal constituency surveillance* (scrutiny of insiders as with work monitoring) contrasts with *external constituency surveillance* (attending to outsiders such as customers, patients, and travelers). *External nonconstituency surveillance* involves organizations monitoring their broader environment in watching other organizations and social trends. The rapidly growing, understudied field of business intelligence fits here.

In *nonorganizational surveillance* the watching is apart from a formal organizational role. It may involve *role relationship surveillance* as with family members (parents and children, the suspicious spouse) or friends looking out for and at each other (e.g., monitoring location through a cell phone). Or it can involve *non-role relationship surveillance* – as with the free-floating activities of the voyeur whose watching is unconnected to a legitimate role.

Agent-initiated surveillance illustrated by compliance checks such as an inspection of a truck or a boat is distinct from *subject-initiated surveillance* – as with volunteering to participate in consumer reward programs. The agent and subject of surveillance can merge with *self-surveillance* – where individuals watch themselves (home alcohol or reproductive tests).

While distinct, subject and agent can be intertwined, as with parallel or *co-surveillance* (e.g., remote health monitoring in which both the monitored person and a health agency simultaneously receive signals about the subject). In the latter case co-surveillance is *nonreciprocal* with personal data from the watched going to the watcher. This tends to be the case with employers, merchants, doctors, teachers, and parents and reflects power and resources differences. In contrast, *reciprocal surveillance* is by definition bidirectional, as with social networking sites. But reciprocal, need not mean equal. Surveillance that is reciprocal may be *asymmetrical* or *symmetrical*. In a democratic society citizens and government engage in reciprocal but distinct, and shifting forms and degrees of mutual surveillance. These questions draw attention to who is entitled to and/or able to play the agent role and who is the subject? New tools may bring increased democratization (or a better term – equalization) as with readily available cell phone cameras and Internet access or the tools may be restricted as with access to satellites, private databases, and sophisticated data mining.

A measure of democracy is the extent of restrictions on and mandatory requirements for information flows across actors and sectors. For example, what is the ratio over time of what governments and large organizations are expected to (or may) reveal about themselves (e.g., freedom of information, truth in advertising laws and policies, and conflict of interest statements) and what citizens are expected to reveal about

themselves to governments and large organizations. Contrast the extremes of a *totalitarian government* that has no obligation to reveal anything to citizens (who must reveal all to government), with the unrealistic case of a *fully open government* that must reveal all to citizens (who in turn reveal only what they choose to government).

The concepts above emphasize structure (i.e., patterned forms of behavior and organization). Structure implies that the topic is static and fixed at one point in time, yet surveillance also needs to be viewed as a fluid, ongoing process involving interaction, strategic calculations, and negotiations over time. Among major processes are the *softening of surveillance* (in which minimal invasiveness, manipulation, persuasion, and low visibility replace traditional coercion); efforts to create the *myth of surveillance* (generating fears supportive of the need for increased surveillance and/or claims that the solution is more effective than it is); the *monetarization* of personal data so it can be sold to marketers, governments, and individuals for purposes of sorting and the *commodification* of surveillance in which it (or protection from it) become products to be purchased; *surveillance slack* – the relative gap between potentials and practices; and various techniques of neutralization. The latter are strategic moves by which subjects of surveillance seek to subvert the collection of personal information such as direct refusal, discovery, avoidance, switching, distorting, counter-surveillance, cooperation, blocking, and *masking*. Equivalent counter-neutralization moves by agents are also present (Marx, 2003).

Another way to think about process is to consider the links between the distinct activities covered by the umbrella term surveillance. The most common meaning refers to acts of data collection, but these occur within a broader system of connected activities. Seven kinds of activity conceived as *surveillance strips* can be noted: *tool selection*, *subject selection*, *collection*, *processing/analysis*, *interpretation*, *uses/action*, and *data fate*. Considered together these strips constitute the *surveillance occasion* and offer a way to bind a given application.

Viewing surveillance in stages also permits us to see one link between *surveillance* and *communication* – the two related topics that are rarely connected. However, at the use stage suggested above surveillance results can be used for targeted marketing, solicitation, and propaganda (Gandy, 1993). Both can involve the crossing of personal borders and respect for, or the disavowal of, a person's dignity – in one case to take from and in another to impose upon, the person in contexts of roles, rules, and expectations. They also share some issues of interpretation and meaning regarding the data surveillance collects and the content of a message.

The 'career' of a particular surveillance tool may also be tracked as it emerges and then may diffuse – whether in a jagged or in a more linear direction. In the case of the latter this may be through *surveillance creep* or *gallop*, often displacing other means along the way and bringing new goals and users. There may also be *surveillance constriction* as a new, unregulated tactic becomes subject to limitations and even prohibitions. Thus, the rampant surveillance that computerization and related forms of electronic monitoring and communication made possible has been somewhat curtailed by laws and policies. An early example was the Electronic Privacy Protection Act of 1986 or with the new concerns that DNA brought the 2008 Genetic Information Nondiscrimination Act. Robert Smith (2013) reports on the vast expansion of state and federal laws regarding surveillance and privacy.

Understanding Surveillance and Value Conflicts

There are many ways of approaching surveillance from the social sciences, and the perspective and methods chosen need to reflect specific questions and local situations (e.g., How were suspects identified before photography was invented?, What are the most important causes of the emergence of a surveillance society?, and Do young people differ in their assessment of the privacy implications of social media from older people?) However, regardless of the kind of question, our understanding will benefit from awareness of factors such as the level of analysis and conflicts in values discussed next.

Understanding surveillance will be furthered to the extent that we:

1. Identify questions and levels of analysis. Central here for both explanation and policy purposes is awareness of social and cultural factors present within different contexts and institutional settings. In addition, how we account for and judge surveillance should depend on the role played and the characteristics of the tool, goals, the kind of data involved, and the values at stake.
2. Identify variation and then look for correlations and explanatory causes/drivers within a framework of soft determinism, but do not confuse correlation with causality.
3. Realize that the same causal factor(s) can have different outcomes and the equivalent outcomes can have different causes.
4. Appreciate the advantages of a loose systems approach with some open-ended borders and room for (but limits upon) exogenous inputs.
5. Attend to beginnings (or at least prior circumstances) – everything was preceded by something before and new ways of meeting human needs must be compared with old ways.
6. Note that while some things change, others remain the same.
7. View surveillance as a process, as well as a structure or a tool. Central to that is studying interactions involving agents, subjects, third parties, and audiences over varying time periods.
8. Ask about the appropriateness of both means and ends. Desirable ends do not justify doubtful means, and good means can be misused. Good goals and purity of motives are not sufficient justification. Consider the acceptability of means and ends independently, as well as in their relationship to each other. Recognize that a given tool can serve a variety of goals and that a given goal can be met by a variety of tools.
9. Differentiate facts from values. No matter how sound the method or clear the findings, a leap to values, ethics, and political choices always remains in what we come to see as facts and in the ends for which surveillance is used.
10. With respect to values (and the goals and specific applications to which they are related) be aware of how their

abstract nature and conflicts between them mean that surveillance will often be subject to legitimate disagreements among well-meaning persons. (The issue of value conflicts is vital and I discuss it in the following paragraphs.)

Value conflicts are everywhere, like the weather. Thus, we seek privacy and often in the form of anonymity, but we also know that secrecy can hide dastardly deeds and that visibility can bring accountability. On the other hand, too much visibility may inhibit experimentation, creativity, and risk taking. And while we value disclosure and 'permanent records' in the name of fairness and just deserts, we also believe in redemption. New beginnings after individuals have been sanctioned, or after they have otherwise overcome limitations or disadvantages, are fundamental to the American reverie.

In our democratic, media-saturated, impression-management societies, many of us want to both see and be seen (e.g., social media) even as we also want to look the other way and be left alone. We may want to know but also be shielded from knowing.

We value freedom of expression and a free press but do not wish to see individuals defamed, harassed, or unduly humiliated (whether by the actions of others or their own). Also as ideals, we desire honesty in communication and also civility and diplomacy. In interpersonal relations (in contrast to the abrasive talk shows) we may work hard to avoid embarrassing others by not seeking certain information or by holding back on what we know. We value the right to know, but also the right to control personal information. The absence of surveillance may bring freedom from censorship, but also open the door to the worst demagogues, liars, and self-deluded snoops. Yet undue surveillance chills nonconforming communication and is the companion of repression.

Individuals expect organizations to treat them in a fair, accurate, and efficient manner, and to judge them as unique, not as undifferentiated members of a general category, while at the same time, they hesitate to reveal personal information and desire to have their privacy and confidentiality protected. Meeting the first set of goals necessarily requires giving up personal data, and up to some point, the more one gives up, the more accurate and distinctly reflective it will be of the unique person. Yet, the more data one reveals, the greater the risk of manipulation, misuse, and privacy violation. At the same time, knowing more can bring new questions and less certainty to surveillance agents. Depending on their role and social location, individuals and groups differ in the relative importance they give to privacy as compared to accuracy.

The individual's expectation to be assayed in his or her full uniqueness may conflict with an organization's preference for responding to persons as part of broad common aggregates – something seen as more rational, effective, and even efficient. The idea of due process and fairness to be determined in each individual case can radically conflict with an organization's utilitarian goals and bottom line. In the criminal justice context, for example, civil liberties sometimes conflict with the goal of effective enforcement. The case for *categorical surveillance* (without cause) versus *particularized surveillance* (only with cause) and for prevention versus after-the-violation responses can be well argued either way.

Culture sends contradictory messages. On the one hand, individuals are expected to submit to surveillance as members of a community that supports the common good and fairness (e.g., the required census or social security number that apply to all) or that allows one to participate in certain behaviors such as traveling, buying on credit, or obtaining an entitlement. Yet fairness apart, when such surveillance goes beyond minimal verification and is done in a coercive manner, it may conflict with the expectation that before personal information borders are crossed, there needs to be some grounds for suspicion. If agents have to wait to do surveillance until they have cause in situations where there is evidence of preparatory actions or where violations are of low visibility or hidden outright, many violators get a free ride. This limitation protects the innocent against unnecessary searches. Yet, it can also mean failing to prevent terrible events – for example, in the case of 9/11, where well-intentioned policies from another era as well as many informal factors blocked the FBI and CIA from exchanging information about the perpetrators.

If your tools work and if you search them all, you will likely get the guilty, not to mention the innocent and this is likely inefficient. Profiling as a surveillance tool permeates society far beyond ethnicity, religion, or national origin. In contemporary society, with its emphasis on prevention, the push is toward broader and deeper searching for the absent cause. The dilemma can be identified but not solved because observers differ in judging the trade-offs between equality, fairness, grounds for suspicion, invasiveness, prevention and effectiveness and the likelihood and seriousness of risks, and the potential for identifying and remedying failures.

The existence of practices with a good potential for abuse traditionally leads to demands for regulation. Thus, we see bureaucratic and legalistic responses. These may lessen problems, but ironically, can also lead to expanded use of potentially troubling means. In contrast, without a formal mandate legitimating and acknowledging the tactic, agents may hesitate to use it because of uncertainty about where to draw the lines.

The above discussion involves conflicts between abstract values. But more concrete conflicts may also appear in applying the tools. The intrinsic properties of a device may work against the agent's desire for secrecy. While much contemporary surveillance is defined by its ability to root out the unseen and unknown, it also paradoxically may reveal itself through electrical, chemical, and other forms of data. That which silently gathers the emanations of others, if not exactly a mirror image, nonetheless emanates itself, offering discovery possibilities and means of neutralization to technically competent adversaries. The watchers may also be watched by the means they apply to others. Also, if an agency publicizes a surveillance system that has as one goal, making citizens feel more secure, it may in addition have the opposite effect because it sends the message that dangers are so great as to warrant the need for such a system. Or this same publicity may alert committed malefactors to the presence of surveillance, triggering evasive, blocking, or displacement means – a kind of unfair (at least to the law-abiding public) warning. Thus, advertising the means versus keeping them secret highlights the potential conflict of goals between deterrence and apprehension so apparent with undercover work. The existence of practices with a good potential for abuse traditionally leads to demands

for regulation. A bureaucratic and legalistic response may lessen problems, but ironically, it can also lead to expanded use of potentially troubling means. In contrast, without a formal mandate legitimating and acknowledging the tactic, agents may hesitate to use it because of uncertainty about where to draw the lines.

A final mandate: with respect to the significant very complex issues new and old forms of surveillance bring to a democratic society, neither a pessimist nor an optimist be. Unless, of course, your view is based on empirical evidence, and a logical and well developed argument that defines its terms and identifies its background assumptions regarding both values and the empirical workings of the world.

Surveillance practices need to be understood within specific settings in light of history, culture, social structure and the give and take of interaction, and require the appreciation (if not necessarily the welcoming) of the ironies, unintended consequences, and value conflicts that limit the best laid plans. Mushrooms do well in the dark, but so does injustice. Sunlight may bring needed accountability through visibility, but it can also blind and burn.

There is a path, however twisting, changing, and bramble and illusion filled between Tennyson's early nineteenth century optimism, "For I dipt into the future, far as the eye could see, saw the world, and all the wonders that would be (Ricks, 1989) and Einstein's 20th century worry that technological progress can become like an axe in the hand of a criminal" (Folsing, 1998). Yet, hope must trump dread as we keep the faith with respect to both the importance of having a dream and the ameliorative potential of critical analysis. Empirical and scientific knowledge about human and social conditions can result in the improvement of those conditions, or maybe stop them from getting worse.

The study of surveillance is a reminder that while they (whether the state, commercial interests or new, expanding public–private hybrid forms) are watching us, we as citizens must watch them. And as baseball player Yogi Berra said, "you can see a lot by looking." Making surveillance (as with any technology) more visible and understandable hardly guarantees a just and accountable society, but it is surely a necessary condition for one.

See also: Community Supervision and Diversion in the United States; Goffman, Erving (1922–1982); Government Statistics; Governmentality; Internet and Privacy; Power in Society; Privacy: Theoretical and Legal Issues; Surveillance and Privacy, Geography of.

Bibliography

Allen, A., 2007. Privacy Law and Society. West Group.
Ball, K., Haggerty, K., Lyon, D., 2012. Handbook of Surveillance Studies. Routledge, New York.
Bauman, Z., 2000. Liquid Modernity. Polity, Cambridge.
Bentham, J., 1995. Introduction. In: Bozovic, Miran (Ed.), The Panopticon Writings. Verso, London.
Bigo, D., 2006. Globalized (in)Security: the field and the Ban-opticon. In: Sakai, N., Solomon, J. (Eds.), Translation, Biopolitics, Colonial Differences. Hong Kong University Press,, Hong Kong, pp. 109–156.
Blomberg, T., 1987. Criminal justice reform and social control: are we becoming security socitey. In: Lowman, J., Menzies, R.J., Plays, T.S. (Ed.), Transcarceration: Essays in the Sociology of Social Control. Gower Publishing Co., Surrey, England, pp. 218–226.
Bogard, W., 1996. The Simulation of Surveillance: Hyper Control in Telematic Societies. Cambridge University Press, Cambridge.
Boyne, R., 2000. Post-Panopticon. Economy and Society 29 (2), 285–307.
Brodeur, J.P., Leman-Langlois, S., 2006. Surveillance fiction or high policing. In: Haggerty, K., Ericson, R. (Eds.), The New Politics of Surveillance and Visibility. University of Toronto Press, Toronto.
Brin, D., 1998. The Transparent Society: Will Technology Force Us to Choose between Privacy and Freedom? Perseus Book Group, Cambridge, MA.
Browne, S., 2015. Dark Matters: On the Surveillance of Blackness. Duke University Press, Los Angeles, CA.
Buzan, et al., 1998. Security: A New Framework for Analysis. Lynne Reiner, Boulder, CO.
Clarke, R., 1988. Information technology and dataveillance. Communications of the ACM 31 (5), 498–512.
Cohen, S., 1985. Visions of Social Control. Polity Press, Cambridge.
Dandeker, C., 1990. Surveillance, Power, and Modernity: Bureaucracy and Discipline from 1700 to the Present Day. Polity Press, Cambridge.
Decew, J.W., 1997. In: Pursuit of Privacy: Law, Ethics, and the Rise of Technology. Cornell University Press, Ithaca, NY.
Deleuze, G., 1992. Postscript on the societies of control. October 59, 3–7.
David, W., et al., 2010. Safeguards in a World of Ambient Intelligence. Springer, New York.
Folsing, A., 1998. Albert Einstein: A Biography. Penguin Books, New York.
Foucault, M., 1977. Discipline and Punish: The Birth of the Prison. Vintage, New York.
Foucault, M., 1998. The History of Sexuality, vol. 1. Penguin, London.
Gabriel, Y., 2005. Glass cages and glass palaces: images of organizations in image-conscious times. Organization 12 (1), 9–27.
Gandy, O., 1993. The Panoptic Sort. Westview Press, Boulder, CO.
Greenfield, A., 2006. Everyware: The Dawning Age of Ubiquitous Computing. New Riders, Berkeley.
Goffman, E., 1961. Asylums. Anchor Books, Garden City, NJ.
Goffman, E., 1971. Relations in Public. Micro Studies of the Public Order. Basic Books, New York.
Haggerty, K., Ericson, R., 2006. The surveillant assemblage. British Journal of Sociology 51 (4), 605–622.
Haggerty, K., Samatas, M., 2010. Surveillance and Democracy. Routledge, London.
Hardt, M., Negri, A., 2001. Empire. Harvard University Press, Cambridge, MA.
Kelvin, P., 1973. A social-psychological examination of privacy. British Journal of Clinical Psychology 12 (3), 248–261.
Laudon, K.C., 1986. Data quality and due process in large record systems: criminal record systems. Communications of the ACM 29 (1), 4–11.
Lianos, M., 2003. Social control after foucault. Surveillance & Society 1 (3), 412–430.
Lyon, D., 2001. Surveillance and Society: Monitoring Everyday Life, Open University Press, Buckingham and Philadelphia.
Lyon, D., 2007. Surveillance Studies: An Overview. Polity Press, Cambridge, England.
Lyon, D., Ball, K., Haggerty, K. (Eds.), 2012. International Handbook of Surveillance Studies. Routledge, London.
Mann, S., Nolan, J., Wellman, B., 2003. Sousveillance: inventing and using wearable computing devices for data collection in surveillance environments. Surveillance & Society 1 (3), 331–355.
Manning, P., 2008. A view of surveillance. In: Leman-Langlois, S. (Ed.), Technocrime: Technology, Crime, and Social Control. Willan Publishing, Devon, UK, pp. 209–242.
Marx, G.T., June 1985. The Surveillance Socitey. The Futurist XIX(3).
Marx, G.T., 2001. Murky conceptual waters: the public and the private. Ethics and Information Technology 3 (3), 157–169.
Marx, G.T., 2003. A tack in the shoe: neutralizing and resisting the new surveillance. Journal of Social Issues 59 (2).
Marx, G.T., 2011. Turtles, firewalls, scarlet letters and vacuum cleaners: rules about personal information. In: Aspray, W., Doty, P. (Eds.), Making Privacy. Scarecrow Press.
Marx, G.T., 2015 Windows into the Soul: Surveillance and Society in an Age of High Technology. University of Chicago Press, Chicago.
Mathiesen, T., 1997. The viewer society: Michel Foucault's 'panopticon' revisited. Theoretical Criminology 1 (2), 215–234.
Michael, M., Fusco, S., Michael, K., 2008. A research note on ethics in the emerging age of uberveillance. Computer Communications 31 (6), 1192–1199.
Monaghan, P., 17 March 2006. Watching the watchers. Chronicle of Higher Education 52 (28), 1 and 18–25.
Monahan, T., 2010. Surveillance in the Time of Insecurity. Rutgers University Press, New Brunswick.

Newman, O., 1972. Defensible Space: Crime Prevention through Urban Design. Macmillan Books, New York.
Nissenbaum, H., 1998. Protecting privacy in an information age: the problem of privacy in public. Law and Philosophy 17, 559–596.
Nogala, D., 1995. The future role of technology in policing. In: Brodeur, Jean-Paul (Ed.), Comparisons in Policing: An International Perspective. Aldershot, Avebury, UK, pp. 191–210.
Norris, C., Armstrong, G., 1999. The Maximum Surveillance Society: The Rise of CCTV. Oxford University Press, New York.
Palidda, S., 1992. L'anamorphose de l'État-Nation: le cas italien. Cahiers internationaux de sociologie 269–298.
Poster, M., 1990. The Mode of Information: Postculturalism and Social Context. University of Chicago Press, Chicago.
Ricks, C., 1989. Tennyson: a Selected Edition. University of California Press, Berkeley, CA.
Rule, J., 1973. Private Lives, Public Surveillance. Allen-Lane, London.
Rule, J., MCadam, D., Stearns, L., Uglow, D., 1980. The Politics of Privacy. New American Library, New York.
Sartre, Jean-Paul, 1993. Being and Nothingness. Washington Square Press, New York.
Smith, R.E., 2013. Compilation of State and Federal Privacy Laws. The Privacy Journal, Providence, RI.
Torpey, J., 2007. Through thick and thin: surveillance after 9/11. Contemporary Sociology 36 (2), 116–119.
Westin, A., 1967. Privacy and Freedom. Columbia University Press, New York.
Wright et al., 2008. Safeguard in a World of Ambient Intelligence. Springer, Dordrecht.