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