Surveillance & Society 1(1): 9-29
www.surveillance-and-society.org

What's New About the "New Surveillance"? Classifying for Change and Continuity*

Gary T. Marx[1]

Abstract

A critique of the dictionary definition of surveillance as "close observation, especially of a suspected person" is offered. Much surveillance is applied categorically and beyond persons to places, spaces, networks and categories of person and the distinction between self and other surveillance can be blurred. Drawing from characteristics of the technology, the data collection process and the nature of the data, this article identifies 28 dimensions that are useful in characterizing means of surveillance. These dimensions highlight the differences between the new and traditional surveillance and offer a way to capture major sources of variation relevant to contemporary social, ethical and policy considerations. There can be little doubt that major changes have occurred. However the normative implications of this are mixed and dependent on the technology in question and evaluative framework. The concept of *surveillance slack* is introduced. This involves the extent to which a technology is applied, rather than the absolute amount of surveillance. A historical review of the jagged development of telecommunications for Western democratic conceptions of individualism is offered. This suggests the difficulty of reaching simple conclusions about whether the protection of personal information is decreasing or increasing.

"We are at any moment those who separate
the connected or connect the separate."
Georg Simmel

Introduction

In an interview with the individual responsible for an all-purpose student id access card used for building entrance, the library, meals and purchases at a large Southern university I encountered the following case:

> The registrar came into his office and discovered an arson effort that failed. A long burn mark on the carpet led to a Gatorade bottle full of flammable liquid in a closet. In an adjacent building police found the area where the bomb was assembled. They requested card access records for

* This article draws from a forthcoming book: *Windows Into the Soul: Surveillance and Society in an Age of High Technology*, based on the Jensen Lectures for Duke University and the American Sociological Association. Additional articles are at: www.garymarx.net/

[1] Professor Emeritus, Massachusetts Institute of Technology, e-mail: gtmarx@bainbridgeisland.net

 ISSN: 1477-7487

> that building. A review of the logs found some early morning card swipes which looked suspicious. They also checked the lot number on the Gatorade bottle that was holding the liquid and determined it had been delivered to a campus convenience store. Upon matching the records of purchasers of Gatorade with those entering the building where the bomb making materials were found, the police got a hit. They confronted the suspect and he confessed to arson. His motive was to burn up his academic records, as he was failing several classes and didn't want to disappoint his parents.

This high tech discovery of human spoors needs only to be bolstered by a video camera, DNA matching and thermal lie detection to serve as a paradigmatic case of the "new surveillance" (Marx 1988). New technologies for collecting personal information which transcend the physical, liberty enhancing limitations of the old means are constantly appearing. These probe more deeply, widely and softly than traditional methods, transcending natural (distance, darkness, skin, time and microscopic size) and constructed (walls, sealed envelopes) barriers that historically protected personal information.

The social causes and consequences of this are profound and only beginning to be understood. These involve broad changes in economic and social organization, culture and conceptions of freedom and constraint. In the overcrowded and overlapping worlds of academic journals, one focusing on Surveillance and Society has a most welcome niche.

The last half of the 20th century has seen a significant increase in the use of technology for the discovery of personal information. Examples include video and audio surveillance, heat, light, motion, sound and olfactory sensors, night vision goggles, electronic tagging, biometric access devices, drug testing, DNA analysis, computer monitoring including email and web usage and the use of computer techniques such as expert systems, matching and profiling, data mining, mapping, network analysis and simulation. Control technologies have become available that previously existed only in the dystopic imaginations of science fiction writers. We are a surveillance society. As Yiannis Gabriel (forthcoming) suggests Weber's iron cage is being displaced by a flexible glass cage.

Three common responses to changes in contemporary surveillance technology can be noted. One general historical and functional view holds that there is nothing really new here. All societies have certain functional prerequisites which must be met if they are to exist. These include means for protecting and discovering personal information and protecting social borders. Any changes are merely of degree, not of kind.

An opposing, less general view is that we live in a time of revolutionary change with respect to the crossing of personal and social borders. There are two variants of this. One is that the sky is indeed falling and, "you never had it so bad". Some journalists and popular writers claim "privacy is dead".

A related view holds that while the technologies are revolutionary, the way they are used reflects social and cultural factors. In that regard the forces of modernity operate to extend individual control. The trend on balance, whether through counter-technologies or changing customs, policy or law, is for protection of personal information to become stronger as new threats appear, although given the piecemeal approach to privacy legislation in the United States (in contrast to that in much of Europe in which protections are based on a broad principle such as "respect for human dignity"), there is usually a lag.

Yet simple sweeping assertions about such a complex, dynamic and varied topic are not very helpful. Broad concepts may in Neil Smelser's (1959: 2) words "shroud a galaxy of connotations". However useful as an intellectual shorthand, ideal types such as "developed vs. undeveloped nations" or "traditional vs. the new surveillance" must be considered in light of the multiple dimensions which usually run through them.

The academic literature on particular surveillance technologies is gradually expanding.[2] In contrast this article offers a minimalist rendering of the most basic dimensions which cut across and can be used to characterize any surveillance activity. It is at the middle range, situated (and offering a bridge) between more abstract theoretical explanations and empirical description. As a prelude to specifying dimensions let us note some shortcomings of popular definitions.

A Deficient Definition

One indicator of rapid change is the failure of dictionary definitions to capture current understandings of surveillance. For example in the *Concise Oxford Dictionary* surveillance is defined as "close observation, especially of a suspected person". Yet today many of the new surveillance technologies are not "especially" applied to "a suspected person". They are commonly applied categorically. In broadening the range of suspects the term "a suspected person" takes on a different meaning. In a striking innovation, surveillance is also applied to contexts (geographical places and spaces, particular time periods, networks, systems and categories of person), not just to a particular person whose identity is known beforehand.

The dictionary definition also implies a clear distinction between the object of surveillance and the person carrying it out. In an age of servants listening behind closed doors, binoculars and telegraphic interceptions, that separation made sense. It was easy to separate the watcher from the person watched. Yet self-monitoring has emerged as an important theme, independent of the surveilling of another. In the hope of creating self-restraint, threats of social control (i.e.: the possibility of getting caught) are well-publicized with mass media techniques.

[2] See for example: Gilliom, 2001; Cole, 2001; Caplan and Torpey, 2001; Nippert-Eng, 1997; Nelkin and Tancredi, 1994; Smith, 1994; Gilliom, 1994; Gandy, 1993; Laudon, 1986; Marx and Reichman, 1984; Rule, 1973. Also the general treatments by: Gutwirth, 2002; Garfinkle, 2000; Rosen, 2000; Smith, 2000; Froomkin, 2000; Etzioni, 1999; Brin, 1998; Ericson and Haggerty, 1997; Staples, 1997; Allen, 1988; Bogard, 1996; Lyon and Zureik, 1996; Lyon, 1994; Allen, 1988.

A general ethos of self-surveillance is also encouraged by the availability of home products such as those that test for alcohol level, pregnancy, menopause and AIDS. Self-surveillance merges the line between the surveilled and the surveillant. In some cases we see parallel or co-monitoring, involving the subject and an external agent.[3] The differentiation of surveillance into ever more specialized roles is sometimes matched by a rarely studied de-differentiation or generalization of surveillance to non-specialized roles. For example regardless of their job, retail store employees are trained to identify shoplifters and outdoor utility workers are trained to look for signs of drug manufacturing.

The term "close observation" also fails to capture contemporary practices. Surveillance may be carried out from afar, as with satellite images or the remote monitoring of communications and work. Nor need it be close as in detailed – much initial surveillance involves superficial scans looking for patterns of interest to be pursued later in greater detail.

The dated nature of the definition is further illustrated in its seeming restriction to visual means as implied in "observation". The eyes do contain the vast majority of the body's sense receptors and the visual is a master metaphor for the other senses (e.g., saying "I see" for understanding or being able to "see through people").[4] Indeed "seeing through" is a convenient short hand for the new surveillance.

To be sure the visual is usually an element of surveillance, even when it is not the primary means of data collection (e.g., written accounts of observations, events and conversations, or the conversion to text or images of measurements from heat, sound or movement). Yet to "observe" a text or a printout is in many ways different from a detective or supervisor directly observing behavior. The eye as the major means of direct surveillance is increasingly joined or replaced by hearing, touching and smelling.[5] The

[3] The self-restraint and voluntary compliance favored in liberal democratic theory receives a new dimension here. The line between the public and the private order maintenance becomes hazier. The border may be blurred in the sense that there can be a continuous transmission link between sender and receiver as with brain waves or scents. Other broken and reconstructed borders are discussed in Marx, 1997. Consider also a federally funded "Watch Your Car" program found in 11 states in 2001. In this program vehicle owners attach a decal to their car inviting police to pull them over late at night to be sure the car is not stolen.. To the extent that this "co-production" of social order becomes established it is easy to imagine individuals wearing miniature video, audio, location and biological monitors sending data outward to protective sources. New borders and forms of neutralization will of course appear, but it will be a new senses-transcending ball game and we will become more aware of the extent to which the limits of the physical world shape cognition and norms.

[4] William Holden nicely captures this in his self-analysis in the film *Picnic*, "What's the use, baby? I'm a bum. She saw through me like an x-ray machine."

[5] Taste is the most under-utilized of the senses for surveillance. Drug agents sometimes taste a suspect substance. I don't know about the validity of biting a stone to determine if it is a diamond (technically this may be closer to feel than to taste but doesn't fit either that well. It involves cognition). Historically the tasters who sampled the food and drink of elites to see if they were poisoned are one example I will learn more about. Evaluating the performance of a chef by tasting the product, a chef's self-monitoring by sampling a dish before serving and a baking contest in which there is a taste test are other examples.

use of multiple senses and sources of data is an important characteristic of much of the new surveillance.

A better definition of the new surveillance is the use of technical means to extract or create personal data. This may be taken from individuals or contexts. In this definition the use of "technical means" to extract and create the information implies the ability to go beyond what is offered to the unaided senses or voluntarily reported. Many of the examples extend the senses by using material artifacts or software of some kind, but the technical means for rooting out can also be deception, as with informers and undercover police. The use of "contexts" along with "individuals" recognizes that much modern surveillance also looks at settings and patterns of relationships. Meaning may reside in cross classifying discrete sources of data (as with computer matching and profiling) that in and of themselves are not of revealing. Systems as well as persons are of interest.

This definition of the new surveillance excludes the routine, non-technological surveillance that is a part of everyday life such as looking before crossing the street or seeking the source of a sudden noise or of smoke. 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.[6]

I do not include a verb such as "observe" 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 I prefer "attend to" or "to regard" rather than observe with its tilt toward the visual.

While the above definition captures some common elements among new surveillance means, contemporary tactics are enormously varied and would include:

- a parent monitoring a baby on closed circuit television during commercials or through a day care center webcast;
- a data base for employers containing the names of persons who have filed workman compensation claims;
- a video monitor in a department store scanning customers and matching their images to those of suspected shoplifters;
- a supervisor monitoring employee's e-mail and phone communication;
- a badge signaling where an employee is at all times;
- a hidden camera in an ATM machine;

[6] However applying a polygraph to an uncooperative subject or for verification purposes, or using a telephoto lens to capture and record an image from far away would fall within the definition. The exposure (if that is the term) volunteered by those at the nude beach is presumably intended to be available only momentarily to the unaided senses of others in the immediate vicinity. To record images or observe from far away introduces considerations of the new surveillance

- a computer program that monitors the number of keystrokes or looks for key words or patterns;
- a thermal imaging device aimed at the exterior of a house from across the street
- analyzing hair to determine drug use;
- a self-test for level of alcohol in one's system;
- a scanner that picks up cellular and cordless phone communication;
- mandatory provision of a DNA sample;
- the polygraph or monitoring brain waves to determine truthfulness;
- Caller ID

Dimensions of Surveillance

To note that the above are examples of new forms of surveillance tells us rather little, even if such laundry lists drive journalistic engines. Nor is the most commonly used form of classification based on the type of technology (e.g., electronic location monitoring) very helpful. Such general terms can mask differences found within the same family of technologies. This also does not help us see elements that may be shared or absent across technologies – whether traditional or new. Descriptive terms are often emotionally laden (e.g., persons have strong feelings of support or aversion to terms such as drug testing or video surveillance) and that can distort analysis. The social analyst needs frameworks for locating variation which go beyond popular language, even if some call it jargon.

Let us move from these descriptive terms to some more abstract and analytic concepts. There is need for a conceptual language that brings some parsimony and unity to the vast array of both old and new surveillance activities. The logic of explanation proceeds best when it accounts for systematic variation.

Table 1 suggests a number of dimensions for categorizing aspects of surveillance. Of course Occam's razor must be applied deftly. The proliferation of categories must have an end other than itself. One must avoid the danger of making distinctions that only a social scientist could love. But what is life without risk?

A good classification scheme should capture the major differences the researcher thinks are important and be broad enough to encompass all examples (an inclusive general dimension can always be further divided into sub-types). Its application to a given case across observers should be clear. Classification schemes are to be judged by whether or not they are useful given the goals of the researcher.[7] We also hold apart the empirical

[7] If one's goal involves the physical or technical elements rather than the social, different factors than those in these would be emphasized e.g., the type of technology such as optical-imaging, sensor, radiating or nonradiating communications devices, whether or not (and what types) of computer chips are involved, what the energy sources are, ease of manufacturing and impact on the environment. Or if the concern is with a particular goal such as testing for drugs, one would contrast the variety of techniques for doing this. These of course may have social implications (e.g., batteries need to be recharged, sensing chips can be easily hidden, living surveillors give off heat). David Lyon (2001) deals with some related themes in classifying surveillance (e.g., coercive vs. seductive forms). See also Detlef Nogala (1995) for a classification of types

question of whether or not (or under what conditions) the surveillance tactic actually works as claimed.

My goals in classification are to organize the empirical patterns in order to:

1. more systematically contrast surveillance technologies;
2. elaborate on the profound changes in contemporary technologies for collecting and analyzing personal information;
3. specify the variation across time periods, settings and methods that theory needs to account for;
4. offer a more logical grounding for ethical and policy judgments about particular tactics and practices.

The dimensions draw from the characteristics of the technology, the data collection process and the nature of the data. Taken together these variables offer a way of classifying and comparing surveillance. Table 1 highlights differences between the new and traditional surveillance. By reducing the size of the angels or increasing the size of the pin, categories can further proliferate. But these distinctions capture major sources of variation relevant to many social, ethical and policy considerations.

For simplicity I have arranged this largely in a series of discrete either/or possibilities (e.g., visible or invisible, gathered by a human or a machine). But there may be continuous gradations between the extreme values (e.g.: between visible and invisible). Some dimensions involve mutually exclusive values (e.g.: single vs. multiple measures) but many do not (e.g.: the hybrid case of a guard dog wearing a tiny video camera).

In some cases classification reflects an inherent property of the technology (e.g., infra-red and sound transmission devices go beyond the unaided senses). In other cases where a means is classified depends on how it is used. A technology may seem to lend itself well to a value (e.g.: video lens can be used invisibly relative to the traditional bulky 35mm camera), but a policy announcing that a video camera is in use would lead to its' being classified as visible.[8]

The differences between traditional and new surveillance can be approached in terms of the categories in Table 1. Traditional surveillance tends to be characterized by the left side of the table. The traditional means have certainly not disappeared. They have however been supplemented by the new forms which tend to fall on the right side of the table.

I don't claim that the values on the right side of the table cleanly and fully characterize every instance of contemporary surveillance that has appeared since the development of the microchip and advances in microbiology, artificial intelligence, electronics, communications and geographic information systems. Nor do the values on the left side

---

of police technology based on goals and functioning

[8] However in this example a general announcement need not necessarily indicate where the camera is. The situation is similar to employers announcing that they use "secret shoppers" to test employees.

perfectly apply to every instance of the old surveillance prior to this. Social life is much too messy for that. There is some crossing over of values (e.g.: informers, a traditional form, have low visibility, drug testing a new form is discontinuous). These are after-all ideal types whose virtue of breadth often comes with the vice of combining elements that show significant variation at a less abstract level. But if the categories are useful in analyzing big variation (or more useful than the descriptive ad hoc naming we presently have), they will have done their job.

The broader project from which this article is drawn is drenched in empirical examples. For limitations of space, here I offer only a summary of the new and traditional surveillance in the abstract terms of Table 1. The dimensions emphasize elements that I think have changed. I thus exclude other very important dimensions useful for comparing types of surveillance apart from the issue of changes. These include the extent of deception and ease or difficulty of neutralizing a technique, factors which appear not to have changed significantly over the last century. I also exclude others such as degree of invasiveness and validity about which the evidence of change is mixed.

The new surveillance relative to traditional surveillance extends the senses and has low visibility or is invisible. It is more likely to be involuntary. Data collection is often integrated into routine activity. It is more likely to involve manipulation than direct coercion. Data collection is more likely to be automated involving machines rather than (or in addition to) involving humans. It is relatively inexpensive per unit of data collected. Data collection is often mediated through remote means rather than on scene and the data often resides with third parties. Data is available in real time and data collection can be continuous and offer information on the past, present and future (ala statistical predictions). The subject of data collection goes beyond the individual suspect to categories of interest. The individual as a subject of data collection may also become the object of an intervention. There may be only a short interval between the discovery of the information and the taking of action.

The new surveillance is more comprehensive often involving multiple measures. But since it is often mediated by physical and social distance (being more likely to be acontextual) it is not necessarily more valid. It is more intensive and extensive. The ratio of what the individual knows about him or herself relative to what the surveilling person knows is lower than in the past, even if objectively much more is known. Relative to the past the objects of surveillance are more likely to be an anonymous individual, a mass or an aggregate. The emphasis is expanded beyond the individual to systems and networks. The data often goes beyond direct representation to simulation and from narrative or numerical form to also include video and audio records. The monitoring of specialists is often accompanied (or even replaced) by self-monitoring. It is easy to combine visual, auditory, text and numerical data and to send and receive it. It is relatively easier to organize, store, retrieve and analyze data. Traditional surveillance is the reverse of the above.

The Talmud states, "for instance is not proof". In contrasting traditional and new forms of surveillance in light of these categories I am convinced that significant change has

occurred. Yet given the breadth of the net cast and limited resources, this has been argued by illustration. A next step is to operationalize concepts and collect quantitative measurements.

Given the nature of perception, lists imply an egalitarianism among terms that is often unwarranted. The dimensions in Table 1 are hardly of equal significance. They can be clustered or ranked in various ways. Among those on the new surveillance side with the clearest social implications are extending the senses, low visibility, involuntary nature, remoteness, and lesser cost. These create a potential for a very different kind of society and call for stringent vigilance. In extending the senses (the ability to see in the dark, into bodies, through walls and over vast distances etc.) they challenge fundamental assumptions about personal and social borders (these after all have been maintained not only by values and norms and social organization, but by the limits of technology to cross them). Low visibility and the involuntary and remote nature of much contemporary surveillance may mean more secrecy and lessened accountability, less need for consent and less possibility of reciprocity. Lesser costs create a temptation to both widen the net and thin the mesh of surveillance. For example what if brain scan technology lives up to the claims of its advocates to identify what people feel, know or are thinking? (New York Times, 9 Dec., 2001) In the interest of preventing terrible things from happening (which after all it would be irresponsible not to do, not to mention legal liability), the sacred value traditionally placed on interior life would be eroded.

Commonalties across Societies and Time Periods?

Of course whether one sees difference or similarity, rupture or continuity, qualitative or merely quantitative change is conditioned by the level of abstraction. Viewed very abstractly, qualitative changes are rare given the constants (both common needs and resource restrictions) and the influence of tradition in human societies. Generally the more fine-grained the analysis, the easier it is to see differences, or in this case, changes.

Societies show a significant degree of cultural continuity as the past informs the present and the present must work with the basic and largely unchanging elements of natural, social and biological systems.[9] Regardless of the society, time period, or institutional area, there will be parallels and functional equivalents.

Information boundaries and contests are found in all societies and beyond that in all living systems. (Beniger, 1986) Humans are curious and to survive individuals and groups must engage in surveillance and protect their borders. A degree of information protection and technology-enhanced (whether science or magic based) efforts to go beyond sensory impressions likely characterizes all societies. But such a vapid assertion can not capture the profound emotional experience of change (and often affront and

[9] Technology of course may push these limits redefining the meaning of life, overcoming gravity and permitting us to see in the dark. A part of genius as well as insanity is in not "accepting" supposedly inherent limits.

invasion) many individuals feel in the face of the new surveillance, nor does it help in understanding variation across contexts.

Means matter and are not simply reactive. Function or need is not the same thing as structure or means. Granted there are some common needs, yet these can be met in very different ways with different consequences. I don't think we gain a great deal by noting that trial by ordeal, torture, the polygraph, and DNA analysis are all means of gathering information and assessing truth claims. Nor are we helped much by seeing that at some level intercepting a cellular telephone message is equivalent to one group reading another's smoke signals. If one wishes to understand a given form in its context and its relation to the culture and social structure in question, to reach moral conclusions and to seek answers via analyzing variation across settings, such commonalties are thin gruel indeed.

Many needs are hardly cast in bronze. Changes in physical conditions such as climate or social conditions – the rise of urban and later industrial societies – may generate new needs and new means to obtain them. For example a mass society with national borders needs to identify and determine the reputation of strangers and validate claims to identity and competence, as well as eligibility for government services.

New means, beyond meeting old needs and appearing in response to new needs, may play an independent role. In considering questions of invention, whether social or material, new means may generate new needs and in a seldom-recognized process may even determine ends, apart from strains originating elsewhere. The push from possibility may lead to a redefinition of, or re-prioritizing of need. This can be aided by the advocacy of entrepreneurs and activists stressing the benefits of applying a favored technology. For example with respect to both health and crime control, the new goal of prevention or risk avoidance has become increasingly important as scientific means have developed, making early identification possible, particularly on a broad aggregate basis. The efficiency and relatively low cost of categorical mass data collection seems to be eroding the value of individualized suspicion, although not without struggle.

Even if surveillance by definition always involves the quest for information, considered concretely, the way it is gathered and the specific goal and content vary enormously within and across societies. Apart from the new mechanisms, the content and predominant forms of surveillance have significantly changed over the last five centuries.

Changes in Content and Form

In the fifteenth century religious surveillance was a powerful and dominant form. This involved the search for heretics, devils and witches, as well as the more routine policing of religious consciousness, ritual and religiously based rules such as those involving adultery and wedlock and keeping basic records of births, marriages, baptisms and deaths. While this continued for several more centuries, its' significance gradually declined.

In the 16th and 17th centuries, with the appearance and growth of the embryonic nation-state which had both new needs and a heightened capacity to gather and use information, political surveillance became increasingly important relative to religious surveillance. The slow spread of a scientific world-view and protections for religious dissent weakened the latter.[10]

Over the next several centuries there was a gradual move to a broadly "policed" society in which agents of the state, industry and commerce came to exercise control over ever-wider social and geographical areas (Silver, 1969; Shils, 1975; Foucault, 1977; Fogelson, 1977; Nisbet, 1977; Fijnaut and Marx, 1995; Ericson and Haggerty, 1997; Deflem, 2000).[11]

We see the gradual and continuing expansion, systematization and scientification of police (and more generally state and market) observation and detection. For the state beyond enhanced informing and infiltration, this involved the creation of specialized units and an expanded census, improved record keeping, police registers and dossiers, identity documents (including those based on biometrics) and inspections. These forms blurred the line between direct political surveillance and in some ways a more modern and benign, or at least neutral, governance or administration.[12] Personal information came to be collected not only for taxation, conscription, law enforcement and border control (both immigration and emigration), but also to determine citizenship, eligibility for democratic participation and in social planning.

In the 19th and 20th centuries with the growth of bureaucracy and the regulated and welfare states, the content of surveillance expanded yet again to detailed personal information in order to determine conformity with an ever-increasing number of laws and regulations and eligibility for various welfare and intervention programs – from social security to the protection of children and animals. A state bureaucratically organized around the certification of identity, experience and competence is dependent on the collection of personal information. Risk assessment, prediction, prevention and rational planning also require such information. Government uses in turn have been supplemented (and on any quantitative scale likely overtaken) by contemporary work, market place and medical surveillance. The contemporary commercial state is inconceivable without the massive collection of personal data.

---

[10] To be sure religious surveillance in the west has not disappeared. Within sects surrounded by a hostile and tempting world, such surveillance (in the form of inquisitions, self-policing, group confessionals) remains strong –whether involving groups such as the Amish, new age cults or rigidly fundamentalist groups. Theocratic states such as Iran and Afghanistan during the 1990s experienced a resurgence and merging of religious and political surveillance.

[11] This of course extended the values of the center outward. But since conduits carry flows in both directions, this has had mixed consequences and represents much more than a monolithic cultural, social and political imperialism.

[12] However using surveillance to serve the citizenship rights and welfare needs of citizens may serve the political interests of elites by enhancing legitimacy.

The historical summary above documents changes noted by those of the most diverse ideological perspectives from Foucault to Nisbet. What is likely to be disputed is what it means and if it is desirable or undesirable. I will briefly explore one strand of this in looking at changes in telecommunications.

Empowerment, Disempowerment or 'Both'?

It is not easy to reach a conclusion about what the changes in surveillance technology imply for western democratic conceptions of individualism, as expressed in the issue of control over personal information. This recalls a story about a young couple who are very excited bout taking the train for the first time. They arrive at the station and ask the conductor, "Will the train be on time?" He takes out a schedule, studies it for a long time and says, "That depends". They then ask, "What does it depend on?" He then looks at another schedule, looks up and down the track, pauses in deep thought and finally replies, "Well, that depends too". Below I offer a brief history with respect to efforts to intercept and protect telecommunications. Any conclusion as to whether things are getting better or worse with respect to the protection of personal information depends. The scholar's task is to indicate what it depends on.

Looked at broadly across time periods, has the ability to protect forms of electronic communication been increasing or decreasing? It is difficult to say. Almost as soon as the telegraph appeared so did wiretapping and the same holds for efforts to intercept every new form of communication. The absolute amount of intercepted telecommunications has increased as the telephone has become nearly universal and as population and the various forms for communication have increased.

However we do not have adequate information to reach strong conclusions about whether the interception of telecommunications has increased in a relative, as well as an absolute sense, declined or remained roughly constant. An assessment of this would require determining the number of involuntary interceptions as a percentage of all telecommunications. It would be ideal to have this broken down by type –interceptions by domestic law enforcement, by NSA and other domestic and foreign intelligence agencies, by telephone company employees, by employers and by private citizens and by factors such as number of, and length of interceptions and number of persons intercepted. Beyond the use of technical means, it would as well be ideal to have interception data for other forms such as the extent of uninvited listening in on a party-line (when they were in existence) or on an extension or speaker phone.

With recent developments estimates should also include overhearing cordless and cellular conversations and intercepting fax, email and webcam communications. Those making loud use of their cell phones in public also have their conversations partially intercepted (although this is not quite the same since it is more voluntary). The appearance and gradual disappearance of phone booths would also be of interest.

We would also want measures for other aspects of interception beyond direct listening and recording such as for call and trap devices which can be used by law enforcement without a warrant to identify when and what number was dialed. The extent of the use of newer techniques that permit identifying networks of communication beyond the traditional one line to another is also of interest. When a communication has been intercepted whether the content stays secret (as is often the case with intelligence agencies) or becomes public (as is often the case with journalistic snooping on film stars and politicians) would ideally also be considered.

Interception issues apart, these means also have implications for protecting some aspects of personal information. Telecommunications has traditionally offered freedom from visual observation. In permitting interactions on a vastly expanded scale without the need to travel and physical co-presence, they greatly enhanced the ability to communicate, while increasing control over information such as appearance, body language, facial expressions, exact location, who one is with and even who the communicator was.[13] Contrast this with a conversation visible to a third party overheard in a public place such as a restaurant.

Over time, elements of the telephone's intrusive potential were curtailed even as other intrusive potentials appeared. Claims must be time, as well as component specific. For example the eavesdropping potential present when all calls had to be made through an operator (the classic telephone operator of Lily Tomlin) disappeared as automatic switching spread, starting in the 1930s. Greater affluence and technical changes have led to the almost complete disappearance of the party line in which several households shared a phone line and conversations could easily be overheard by just picking up the phone. Initially the service monitoring of phone lines required an operator to listen to conversations can now generally be served by merely checking electronic signals.

While it took almost a century, non-court approved wiretapping eventually was prohibited with the Katz decision (Katz vs. United States, 389 U.S. 347, 1967) which found that there is a right to privacy even in a "public" phone booth. The Court held that the Fourth Amendment applied to persons not to places and to electronic, as well as physical searches. Title III of the 1968 Omnibus Crime Control and Safe Streets Act made unauthorized wiretapping a felony. To judge from impressionistic accounts, the amount of wiretapping without a warrant appeared to have declined after that.

Cordless and cell phone communication, appearing in the 1980s, which rely on radio transmissions were technically easy to legally intercept with scanners and even some UHF television channels. But 1986 legislation made their interception without a warrant illegal. Greater technical protection also came to be built into the phones.

[13] However this may change to the extent that video phones become widespread and manners (or technology) mandate their use. In principle one would be free to choose whether or not to have this and then whether or not to turn it on. Yet subtle and not so subtle social pressures may tilt toward continual use. Lack of reciprocity on an individual's part (failure to use it) may lead the other party to a communication to wonder what the individual is hiding. There is some parallel to expectations about not wearing a mask in face-to-face interactions.

Starting in the 1980s as analogue voice communications carried over copper wires began to be replaced by digital based technologies and services carried on fiber optic wires, interception in principle became easier. Messages whether by phone, fax or e-mail routinely arrived with identifying details that were much more difficult to locate with the analog system. Phone numbers could be automatically linked to reverse directories for additional information. In addition, communication content could be tapped directly through remote computer entries, rather than having to go through the risky procedure of directly tapping into the line at the location of interest. However without appropriate design of the system, locating the actual transmission carrying a message was apparently more difficult. The controversial Digital Telephony Act of 1994 is intended to change that by requiring communications manufacturers to engineer systems that make remote wire tapping easy via computer easy.

However no matter how much more communication there is to intercept, or how much easier it becomes to do, this can be thwarted, or at least inhibited by use of encryption. While it took almost a century, public encryption of telecommunications is now widely available, offering an unprecedented level of communications privacy. On the other hand there are technical efforts via remotely (or directly) planted sniffers to get to a message before it can be encrypted.

The silent recording capability now built into many answering machines makes it easier to secretly record conversations and the marketing to the public of telecommunications surveillance equipment once available only to police may also have increased the interception of communication. However this is matched by the marketing of equipment for protecting communications.

E-mail could be legally intercepted until the passage of the Privacy Protection Act of 1986. The sending of junk fax and automated phone dialing was prohibited not long after. Until the appearance of Caller-ID in 1988, the caller was not required to reveal his or her phone number. Then by technological fiat all callers, even those who were unlisted had their number delivered. This reversed the previous advantage for callers of anonymity and the ability to intrude at will. Caller-ID as initially offered increased the control of the caller, while decreasing control of the person called, since his or her phone number and other information could be involuntarily delivered (and by implication all the other information this can be automatically related to through data bases). Yet several years later a public outcry over Caller-ID led to a blocking option, restoring some of the status quo.

Other forms are more difficult to label as involving an increase or decrease in control. What should we make of the ability to record conversations? On the one hand if this is done secretly and/or against the will of one of the parties, their control is weakened. But if done with their consent, it may increase control by offering a means of validating claims as to what was communicated. This cuts against the natural tilt toward favoring the claims of the more privileged and those of higher status.

Developments such as video phones, internet web transmissions, use of phone technology to transmit biometric data and the merging of the cell phone and still camera further illustrate the dynamic nature of the situation and the mixture of empowering and controlling elements. A central question of course is just who is being empowered or controlled, and for what ends? In the case of Caller-ID is this the caller or recipient of a call, or both relative to third parties? Since all of us play a variety of roles the technology both empowers and lessens power, although hardly to the same degree across roles, institutions and broad contexts.

Within any measure of the amount of personal information collected is the tricky question of the ratio of involuntarily to voluntarily provided information. The new surveillance is of social concern partly because of its ability to gather information secretly and involuntarily. For many observers, if the ratio stays constant or even moves toward an increase in voluntarily provided information, that is progress. As a formal matter, there has never been more informed consent in our society and the amount seems to be increasing. Consider the ratio of voluntarily recorded phone conversations vs. those from wiretaps. Most recorded phone conversations are formally consensual, as with the millions of service calls each day in which persons are told their conversation is being recorded. In most work settings it is also now standard practice to inform employees of the kind of communications monitoring (phone, e-mail etc.) they face.

Yet we must also ask just how "voluntary" such recording is. In principle the individual can always hang up or choose not to work for a super-surveilling employer. Sometimes there is a choice and a request not to record a phone call will be honored. But usually such consent is specious since one needs the service, information or job and just saying "no" denies these. The role of manipulation and deception in obtaining consent also need to be considered, as does the relative ease of consenting (note the contrast between "opt in" and "opt out" systems). Still in general a principle of consent is to be preferred to secrecy and non-consent.

Surveillance Slack

Some aspects of the new surveillance lend support to claims regarding the extension of individualism and the ennoblement of human affairs associated with modernism. Thus the techniques can contribute to restrained and enlightened social control, helping to create a society orderly enough to enjoy its' freedoms. The usual social class implications may even be reversed – those most subject to many forms of the new surveillance are the more privileged who rely so extensively on credit cards, cell phones and computers.

Through offering high quality documentary evidence and audit trails, the new surveillance may enhance due process, fairness and legitimacy. It may contribute to the political pluralism central to democracy by making the tools of surveillance widely available so that citizens and competing groups can use them against each other, as well government, to enhance accountability.[14] In the United States, unlike in many societies, surveillance technology is widely available to the public (even satellite imagery). A

[14] Of course an insecure society in which individuals need to be constantly watching over their shoulder is hardly ideal.

common transmission process is from military to law enforcement to industry to the public at large (e.g., night vision technology, drug testing, the internet). The surveillance may move from being a one-way mirror to being a window.

Another general indicator of progress can be seen in considering the extent of surveillance slack. With sensationalist and often unrepresentative examples, the media talk of the death of privacy with implicit reference to a supposed utopian past and privacy advocates are constantly documenting new risks. In contrast entrepreneurs too often discuss hypothetical benefits of new technologies as if they were fact. In the rhetorical excesses, which shape public awareness, there is a failure to differentiate the potential of a tactic from its actual use. This suggests the need for a broad comparative measure of surveillance slack which considers the extent to which a technology is applied, rather than the absolute amount of surveillance.

We can envision settings in which technology is relatively weak and in which there are few restraints on its application as in Europe in the middle ages. Conversely there are situations in which technology is very powerful, yet there are significant restraints, as with wiretapping in the United States. This contrasts with situations in contemporary authoritarian societies in which the technology is strong and the restraints on it applications are few.

In the United States from the end of the 19th century to the present, the individual's formal rights to, in principle at least[15], control personal information have increased through legislation and judicial rulings with the greater institutionalization of civil liberties and privacy.[16] Organizational policies and counter-technologies have also brought protections.

The ratio between what could be known given the means for discovering personal information and what is actually known was probably much smaller in the 19th century than is the case today and was much smaller still in the middle ages and throughout most of recorded human history. The weakness of the technology was matched by the fact that there was much less to be known about behavior.

In absolute terms, given ways of living and comparing pre-industrial, industrializing and contemporary societies, the amount of personal information that is potentially knowable would seem to have increased markedly over time as societal scale, density, differentiation and formal record keeping increased (e.g: remote communications, the number of people interacted with, geographical mobility etc.)

In the 19th century there was also less physical privacy given smaller living quarters and larger families. The notion of the stifling, fish-bowl environment of the small town is a truism, having been well publicized by escapees to the more anonymous city. The idea of

[15] Practice of course is another matter. Note the frequent misuse of the social security number in spite of restrictive legislation.
[16] On the broader development of individualism and the law see the paper by Wood and Fischer in Alexander, Marx and Williams, forthcoming.

citizenship, labor, consumer and privacy rights were less developed and the borders between work and home or the home and the state were weaker (note the company town and unrestrained police searches).While the technology was weak, there were fewer restraints on its' use and fewer means of neutralizing it.

The surveillance slack measure may be too relativistic for many observers.[17] A lesser evil is still evil and a greater good is not the best. For those in the Biblical tradition of the prophets, or believing in the inevitable cascading of slippery slopes, the only standard is the absolute ideal. To make judgments based on empirical data is irrelevant when the principle is the standard.

In summary even with just one technology such as telecommunications, no simple empirical conclusion can be drawn about whether the control of personal information has increased or decreased. Holding apart crisis periods such as wartime, the pattern is neither consistent over time, nor equivalent across different kinds of personal information or border crossings.[18] How much more difficult then to draw conclusions about improvement across all means of surveillance, particularly in the absence of broad empirical research. Even with an empirical pattern that lends itself to conclusions, the issues of moral evaluation are far from simple.

It is also necessary to consider technologies in relation to each other and in toto. Functional alternatives in which if one way of meeting a goal or need is blocked another will be found, must also be considered. Thus restrictions on wiretapping may result in an increase in the use of informers or undercover operations which are alternative, less restricted means of obtaining information. Or these may increase together as informers' tips are used to justify obtaining wiretaps.[19] Efforts to successfully limit the application of the polygraph through legislation (Regan, 1995) resulted in a decline in its use, but were accompanied by a significant increase in other, even less validated, forms such as paper and pencil honesty tests.

In democratic free market societies along with more powerful technologies, may come counter-technologies and the strengthening of individual rights to protect personal data. Nor are individuals (or groups) simply passive reeds in a technological hurricane. They

[17] The empirical analyst concerned with these issues as a citizen faces a dilemma in that the kind of scholarly analysis suggested here can create undue complacency in the face of potential dangers to liberty. Yet in the long run honesty is a better ally than rhetoric.

[18] In an article that suggests a framework for drawing ethical conclusions I suggest that when violations of personal borders occur this is likely to involve one of four conditions (Marx 1998). For example this may involve a breaching "natural" border presumed to be protective of personal information such as clothes, inner thoughts and feelings, doors, spatial distance, darkness, skin or bodily orifices and directed communication. It can involve a social border where there is an expectation of confidentiality or a spatial or temporal border separating information from various periods or aspects of one's life. It may also involve breaching the tacit assumption that interaction and communication are ephemeral and transitory and not to be captured and preserved through covert means.

[19] This raises an issue of when one technology displaces another, rather than serving to simply pile on what is already there. Gilliom(2001) for example notes that the appearance of an elaborate computerized monitoring system for those on welfare has supplemented rather than displaced the traditional system of "rat calls" as a means of information on violations.

have resources to fight back. (Marx, forthcoming) A dialectical process can often be seen in which changes in behavior patterns and the development of extractive technologies lead to new rules and technologies for limiting their application. Technologies are both determined and determining. They do not enter a neutral culture, but one with informal and formal protections for personal information, as well one with value and organizational supports for collecting such information. Yet, having appeared, their distinctive attributes may have independent and unanticipated impacts.

In the United States, within very broad boundaries over the last century there is something of a moving equilibrium – as the ability to technically cross personal informational borders has increased over time, so has the ability to legally and technically protect personal information.[20] But the road is broad and elastic indeed with respect to both form and time period and the multi-dimensional lines are jagged rather than straight. It is important to appreciate complexity and to be very clear about the frames of reference applied when making either empirical (new or not new, more or less control) or moral (good or bad) claims regarding surveillance developments.

Finally in spite of the social analyst's predilection for noting the constraining elements of social systems, the past needn't be a guide to the future. Powerful forces work against any easy assumption that a decent society is self-perpetuating or that once set in motion, progress must continue. The masthead of a black civil rights newspaper in Sun Flower County, Mississippi reads, "Freedom is a Constant Struggle". This heralds an important truth. There are no permanent victories in the liberties business. Liberty and individualism are fragile and historically the exception rather than the rule. There is no guarantee that hard won rights will stay won or be extended, in the face of continual social and technical challenges. But vigilance, knowledge and wisdom are likely to help.

References

Allen, A. (1988) *Uneasy Access: Privacy for Women in a Free Society.* Totowa, N.J.: Rowman and Littlefield.

Beniger, J. (1986) *The Control Revolution: The Technological and Economic Origins of the Information Society.* Cambridge, Mass.: Harvard University Press.

Bogard, B. (1996) *The Simulation of Surveillance: Hyyper Control in Telematic Societies*. New York: Cambridge University Press.

Brin, D. (1998). *The Transparent Society.* Reading, Ma.: Perseus Books.

[20] There are of course profound conflicts here over the meaning of privacy and the multiple meanings of the terms public and the private. In stressing one rather than another meaning, individuals often talk past each other. Note for example public and private places as geographically defined, public and private information access, customary expectations and manners, the accessibility or inaccessibility of information to the unaided senses, the actual state of information as being publicly known or unknown and social status and roles with differential access to information (Marx, 2001).

Byrne, J. et al (1992) *Smart Sentencing: The Rise of Intermediate Sanctions*. Beverly Hills: Sage.

Caplan, J. and Torpey, J. (2001) *Documenting Individual Identity.* Princeton, N.J.: Princeton University Press.

Cole, S. (2001) *Suspect Identities*. Cambridge, Mass.: Harvard University Press.

Deflem, M. (2000) Bureaucratization and Social Control: Historical Foundations of International Police Cooperation. *Law and Society Review*, 34(3): 601-640.

Ericson, R. and Haggerty, K. (1997) *Policing the Risk Society.* Toronto: University of Toronto Press.

Etzioni, A. (1999) *The Limits of Privacy*. New York: Basic Books.

Fijnaut C. and Marx, G. (1995) The Normalization of Undercover Policing in the West: Historical and Contemporary Perspectives. In Fijnaut and Marx (eds.) *Undercover Police Surveillance in Comparative Perspective.* The Hague: Kluwer Law International.

Fogelson, R. (1977) *Big-City Police*. Cambridge, Mass.: Harvard University Press.

Foucault, M. (1977) *Discipline and Punish: The Birth of the Prison.* New York: Pantheon.

Froomkin, M. (2000) The Death of Privacy? *Stanford Law Review*, 52(5): 1461-1543.

Gandy, O. (1993) *The Panoptic Sort: A Political Economy of Personal Information*. Boulder, Colo.: Westview.

Garfinkel, S. (2000) *Database Nation*. Sebastopol, Ca.: O'Reilly.

Gabriel Y. (forthcoming) The Glass Cage: flexible Work, Fragmented Consumption, Fragile Selves. in J. Alexander, G. Marx, and C. Williams (eds.), *Self, Social Structure and Beliefs: Essays in Honor of Neil Smelser*. University California Press, forthcoming.

Gilliom, J. (2001) *Overseers of the Poor*. Chicago: University of Chicago Press.

Gilliom, J. (1994) *Surveillance, Privacy, and the Law: Employee Drug Testing and the Politics of Social Control*. Ann Arbor: University of Michigan Press.

Laudon, K. (1986) *The Dossier Society.* New York: Columbia University Press.

Lyon, D. (1994) *The Electronic Eye*. Cambridge: The Polity Press.

Lyon, D. (2001) *Surveillance Society: Monitoring Everyday Life.* Buckingham: Open University Press.

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

Marx, G.T. (1997) The Declining Significance of Traditional Borders (and the Appearance of New Borders) in an Age of High Technology. In P. Droege (ed.) *Intelligent Environments.* Amsterdam: Elsevier.

Marx, G.T. (1998) An Ethics for the New Surveillance. *The Information Society*, 14(3): 171-185.

Marx, G.T. (2001) Murky Conceptual Waters: The Public and the Private. *Ethics and Information Technology*, 3(3): 157-169.

Marx, G.T. (forthcoming) A Tack in the Shoe: Neutralizing and Resisting the New Surveillance. *Journal of Social Issues*, Special issues on technology and privacy.

Marx, G.T. and N. Reichman (1984) Routinizing the Discovery of Secrets: Computers as Informants. *American Behavioral Scientist*, 27(4): 423-452.

Nelkin, D. and L. Tancredi (1994) *Dangerous Diagnostics: The Social Power of Biological Information*. Chicago: University of Chicago Press.

Nippert-Eng, C. (1997) *Home and Work: Negotiating Boundaries through Everyday Life.* Chicago: University of Chicago Press.

Nisbet, R. (1977) *Twilight of Authority.* New York: Random House.

Nogala, D. (1995) The Future Role of Technology in Policing. In J. P. Brodeur (ed.) *Comparison in Policing: An International Perspective.* London: Avebury.

Regan, P. (1995) *Legislating Privacy: Technology, Social Values and Public Policy*. Chapel Hill: University of North Carolina.

Rosen, J. (2000) *The Unwanted Gaze*. New York: Random House.

Shils, E. (1975) *Center and Periphery: Essays in Macro Sociology*. Chicago: University of Chicago Press.

Silver, A. (1969) The Demand for Order in Civil Society: A Review of Some Themes in the History of Urban Crime, Police and Riots. In D. Bordua (ed.) *The Police*. New York: Wiley.

Smelser, N. (1959) *Social Change in the Industrial Revolution*. Chicago: University of Chicago Press.

Smelser, N. (1997) *The Problematics of Sociology: The Georg Simmel Lectures*. Berkeley: University of California Press.

Smith, H. J. (1994) *Managing Privacy: Information, Technology and the Corporation*. Chapel Hill: University of North Carolina Press.

Smith, R.E. (2000) *Ben Franklin's Web Site.* Providence, RI: Privacy Journal.

Staples. W. (1997) *The Culture of Surveillance*. New York: St. Martin's Press.

Table 1: ***SURVEILLANCE DIMENSIONS***

DIMENSION	**A. Traditional Surveillance**	**B. The New Surveillance**
Senses	unaided senses	extends senses
Visibility (of the actual collection, who does it, where, on whose behalf)	visible	less visible or invisible
Consent	lower proportion involuntary	higher proportion involuntary
Cost (per unit of data)	expensive	inexpensive
Location of data collectors / analyzers	on scene	remote
Ethos	harder (more coercive)	softer (less coercive)
Integration	data collection as separate activity	data collection folded into routine activity
Data collector	human, animal	machine (wholly or partly automated)
Data resides	with the collector, stays local	with 3rd parties, often migrates
Timing	single point or intermittent	continuous (omnipresent)
Time period	present	past, present, future
Data availability	frequent time lags	real time availability
Availability of technology	disproportionately available to elites	more democratized, some forms widely available

DIMENSION	**A. Traditional Surveillance**	**B. The New Surveillance**
Object of data collection	individual	individual, categories of interest
Comprehensiveness	single measure	multiple measures
Context	contextual	acontextual
Depth	less intensive	more intensive
Breadth	less extensive	more extensive
Ratio of self to surveillant knowledge	higher (what the surveillant knows, the subject probably knows as well)	lower (surveillant knows things the subject doesn't)
Identifiability of object of surveillance	emphasis on known individuals	emphasis also on anonymous individuals, masses
Emphasis on	individuals	individual, networks systems
Realism	direct representation	direct and simulation
Form	single media (likely or narrative or numerical)	multiple media (including video and/or audio)
Who collects data	specialists	specialists, role dispersal, self-monitoring
Data analysis	more difficult to organize store, retrieve, analyze	easier to organize, store, retrieve, analyze
Data merging	discrete non-combinable data (whether because of different format or location)	easy to combine visual, auditory, text, numerical data
Data communication	more difficult to send, receive	easier to send, receive

Return to Dimensions of Surveillance