Know Techn Pol (2007) 20:91–95
DOI 10.1007/s12130-007-9009-5

ORIGINAL PAPER

Privacy and Social Stratification

Gary T. Marx

Received: 15 February 2007 / Accepted: 15 April 2007 / Published online: 2 August 2007

Abstract This article notes ways that power is central to questions of personal information access and use. New surveillance technologies are likely to sustain and even strengthen traditional forms of social stratification. Yet power is rarely a zero-sum game. A number of factors that limit unleashing the full potential of privacy-invading technology, even in contexts of inequality, are considered: legal and moral normative constraints on power holders; the logistical and economic limits on total monitoring; the interpretive, contextual, and indeterminate nature of many human situations; system complexity and interconnectedness; human inventiveness; and the vulnerability of those engaged in surveillance to be compromised or responded to in kind.

Keywords Privacy · Social stratification · Surveillance · Inequality · Sociology of Information · Social issues

Privacy raises many social issues. One insufficiently considered issue involves implications for stratification and equality. The work of Karl Marx, Max Weber, and Michel Foucault on the development of the modern state suggests that inequality is often associated with the use of technologies to collect personal information—whether as a cause or a consequence or both. This may involve monitoring workers, determining the characteristics of those processed and managed by bureaucratic organizations such as the military, police, schools, hospitals, factories and merchants.

The control over information—the defining characteristic of privacy—is a resource related to, but with varying degrees of independence from, other scarce social resources such as class, status, and power. Such resources are the basis for stratification in society.

As computers become ever more important, questions about the extent and consequences of a "digital divide" appear. Is society becoming increasingly stratified on the basis of access to information? Privacy issues are strands of this much broader tapestry.

The connection between knowledge and power is strong, but as with most things social, the correlation is imperfect and depends on the specifics and the context. The ability to define situations regarding what is right and wrong and how people are to be treated obviously involves power. There are times as noted below when the richness and dynamic nature of social reality weakens or reverses the link. Yet on balance differential access to information favors the privileged—whether individuals, groups, countries, or regions.

Rules regarding who can collect personal information, what is collected, the conditions under which it is gathered, and how it is used (and by whom) are very much connected to social stratification. Many contemporary concerns over privacy invasion involve large organizations and their employees and customers, police and suspects, guards and prisoners, and professionals and clients, as well as interpersonal relations as with parents and children. In these contexts the rules are relatively clear about who can ask or observe and who is

G. T. Marx (✉)
Massachusetts Institute of Technology,
77 Massachusetts Avenue,
Cambridge, MA 02139-4307, USA
e-mail: gtmarx@garymarx.net

expected to reveal (or is entitled to conceal). Consider also the extreme imbalance in caste and slave systems. Situations involving power differences with respect to gender and ethnicity may also reflect information inequality.

In these organizational patterns we often see stratification within stratification. The irony of control agents themselves being under surveillance is strengthened by new technologies that indiscriminately record all in their path. Prison guards, for example, are watched and recorded by the same means they use on inmates. In the high visibility conditions of wired shopping malls, guards never know when they are being watched, overheard, or secretly tested.

Coser (1961) uses the felicitous phrase "insulation from observability" to describe the norms and resources that protect the actions of higher status roles in bureaucratic organizations.

Observability is also affected by the extent to which various kinds of personal information are aggregated or compartmentalized. One aspect that is central to contemporary controversies involves the ability to merge distinct data bases by using a universal identifier (whether referring directly to the person's identity, location, or through pseudonymous or anonymous means).

Beyond rules about who can ask or know and who must reveal, the literal availability of physical barriers to visibility needs to be considered. Contrast the enclosed office with soundproof walls that managers may have with the open cubby of office workers. The homeless are "in public" not only because they are on city streets, but because they often lack the insulation of walls or vehicles that prevent observation.

Issues of scale and the extent of geographical dispersion vs concentration in the activities of daily life can also be noted. McCahill (2002) found significant differences in his study of two malls serving lower and higher status groups in England. The first mall was adjacent to a geographically isolated public housing project in which the resources for daily living were highly concentrated. Shops, medical facilities, and government offices were in the mall. In their rootedness and with a lack of insulating resources, residents were under constant surveillance in their daily round when they shopped, saw a doctor, used the post office, made a telephone call, or sat on a bench. In contrast, the more affluent and mobile patrons of the upscale mall had many more options and in some ways greater privacy as a result, e.g., vehicles that made transportation to dispersed services easier, backyards for recreation, phones *within* their homes, and the ability to pay for deliveries.

Some Types of Surveillance

The surveillance that crosses privacy borders can be analyzed with respect to whether it is nonreciprocal or reciprocal. The former is one-way with personal data going from the watched to the watcher (e.g., employers, merchants, doctors, teachers, and parents) and tends to reflect power and resource differences.

In contrast, reciprocal surveillance is bidirectional. But reciprocal, need not mean equal. Thus, in a democratic society citizens and government engage in reciprocal but distinct forms of mutual surveillance. Citizens can watch government through requirements for open hearings and meetings, freedom of information requests, and conflict of interest, and other disclosure statements. However, unlike government, citizens can not legally wiretap, carry out Fourth Amendment searches, or see census or tax returns. Citizens can obtain some information from the public records that corporations must file. The corporation may require citizens to provide personal information in return for goods and services, but it does not offer equivalent information about those within its organization. Patients reveal a great deal to doctors, but beyond seeing framed symbolic diplomas and licenses, generally none are offered the doctor's personal information.

In bounded settings such as a protest demonstration, there may be greater equivalence with respect to particular means, e.g., police and demonstrators may videotape each other, an example of *symmetrical reciprocated* surveillance. This is seen in many settings of organizational conflict in which the contending parties are roughly equivalent. Games such as poker involve this, as do some contractual agreements and treaties (e.g., the mutual deterrence of nuclear arms control sought through reciprocal watching).

Symmetrical forms may be present even in the absence of formal agreements. Spies (or more neutrally, intelligence agents), whether working for countries, companies, or athletic teams, are often mirror images of each other. They offensively seek to discover their opponents' information and defensively to protect their own.

Yet on balance, asymmetry in formal surveillance and information rights within hierarchical organizations and other stratified settings remains. This asymmetry is not always easy to see because it can be embedded in the physical and cultural environment. Imaginative norm-breaching and bending experiments such as those by Mann et al. (2003), who uses a visible webcam to film employees, in stores that themselves are using video cameras to watch customers, can help identify it. In the research of Mann et al. the one-sidedness quickly becomes apparent when, with no appreciation for the humor or irony in the situation, he is told to leave the store.

The development and use of information-avaricious technologies tends to reflect differential access to resources. On the average, privacy-invasive technologies seem more likely to enhance the status quo and to extend inequality than the reverse. The more privileged have an advantage in the development, control, and use of technology.

The use of technologies for social sorting with respect to opportunities for employment, consumption, health care, and the allocation of suspicion are profound (Gandy 1993; Lyon 2003; Lace 2005).

The ability to control information is central to the borders of social groups. Privacy is a social and an individual value (Regan 1995). For example, a legal oppositional political group (or indeed any group) needs to be able to control information about members, resources, and plans and to feel that freedom of expression within the group is respected. To the extent that a group's borders are porous—punctured by informers and intensive surveillance—its ability to act is weakened, and of course democratic ideals are undermined.

Consider the following thought experiment. What if those in developing nations, the colonized, workers, the poor, subordinate ethnic groups, the physically and mentally ill, social service agencies, and those in prison, had the same resources to develop and implement technologies to serve their needs that are available to developed nations, corporations, the military, the police, and corrections? Would we see different technologies and uses? What if the information technology advances of the 1990s and later had been available during the more idealistic and social reform focus of the early and mid-1960s?

Depending on the component, privacy can be either a right to which all citizens are entitled, or a commodity that must be paid for. Responding to demand, the market system increasingly offers technologies and services for protecting personal information—from shredders to tools for finding hidden cameras to home security systems to various software and privacy-protection services. To the extent that privacy comes to be seen as a commodity in which how much you get depends on how much you can (or are willing to) pay; the more privileged are clearly in a better position to obtain it. They are also better situated to avoid being seduced by consumer rewards into voluntarily giving up (in a sense selling) their privacy. Conversely, with greater resources, they can afford to buy personal information about others.

Is Technology Neutral?

George Orwell, the author of the novel *1984*, was once asked, "Isn't technology neutral?" To which he is said to have replied, "Yes, and so is the jungle." Yet as with the animals in another of Orwell's novels, *Animal Farm*, surveillance is more neutral for some than for others.

It is important to acknowledge the sense in which privacy-invasive technologies are (and can be) neutral. Yet the actual use of a technology needs to be considered apart from its *potential* use. Part of the neutrality or equality-of-technology argument is equivalent to Anatole France's observation that the rich and the poor are both forbidden to sleep under bridges or steal a loaf of bread.

Certainly the camera, audio recorder, or motion detector will capture *whatever* is encountered independent of social factors—whether economic level, gender, or ethnicity. This can introduce fairness and help sand some of the rough edges of stratification. The populist arming of subordinates and the public at large with personal computers and recording devices may serve as a counter weight to the surveillance tools of the more powerful (Brinn 1999). Consider the video cam documentation of police abuse seen on the evening news, or being hoist on one's own petard, as in the case of President Nixon and the Watergate tapes.

But this egalitarian potential of the new technology does not mean that all persons and settings have an equivalent chance of being surveilled. Nor are the resources (whether cultural or physical) to defend, resist, and challenge equally distributed in stratified settings and societies. When they are available, their use may be prohibited, as with company policies banning the use of cell phone cameras.

In the prison case noted above, in spite of the omnivorous potential of the lens, there is unlikely to be a camera or audio recording of what goes on in the warden's office or recreational room for guards, nor in the bathroom they use. The inmates' cells have no monitors that permit them to watch the guards, nor can they legally have cell phone cameras or even cell phones.

Complicating Factors

Yet let us note some factors that qualify the familiar connection between privacy and stratification. Conceptions of privacy vary depending on the historical context. The Greeks for example placed the highest value on public life. One's sense of identity was found there. Privacy, being the realm of slaves, women, and children who were restricted to the home, was not valued. To be private meant deprivation. Are there historical referents in the fact that privy is term for a toilet?

But beyond questions of cultural relativism, power is rarely a zero-sum game and there are forces operating to weaken the link between privacy protection and invasion and stratification. The ability to invade privacy as a reflection of power differences is often limited because it is rooted in conflicting values and interdependency and is expressed on a broad and decentralized scale within a free market economy.

A number of factors limit unleashing the full potential of privacy-invading technology, even in contexts of inequality: legal and moral normative constraints on power holders; the logistical and economic limits on total monitoring; the interpretive, contextual, and indeterminate nature of many human situations; system complexity and interconnectedness; human inventiveness; and the vulnerability of those engaged in surveillance to be compromised or responded to in kind.

In spite of doomsday scenarios with respect to the death of privacy and liberty, in societies with liberal democratic economic and political systems, the advantages of technological and other strategic surveillance developments are sometimes short-lived and contain ironic vulnerabilities.

In some ways technologies are neutral and can help or even favor the less privileged. The design of automated and more transparent systems that restrict or eliminate discretion may lessen the potential for official corruption and discrimination. The creation of documentary records of transactions that can later be reviewed (as with audio and video recordings) can offer evidence of what occurred in contested settings. The natural claims—making advantage of the more privileged—may be somewhat offset.

The democratization of privacy invading and privacy-protecting technologies as seen in their widespread availability and ease of application could increase equality. Through *countersurveillance* we see an ironic turning of the tables. Thus, facing a urine drug test, employees can first experiment at home, testing themselves with a variety of readily available products like those used in the official test, or they may protect their private behavior through using products that mask drug residue.

Lower status support persons such as maids, valets, butlers, chauffeurs, or personal assistants are also often required to (or come to) know a great deal about the private lives of those they work for and this tends not to be reciprocated.

In modern societies where the mass media is so central, elite status comes with some new costs. Thus, political leaders and celebrities lack the anonymity of the average person. They both occupationally, and perhaps psychologically, need to be in the public eye, while simultaneously placing a high value on being left alone. The same mass media that is so central to their success also invades their privacy (note the market for the goods of the paparazzi).

But other factors go far beyond public figures. Social life is dynamic. To be modern and successful in contemporary society increasingly means to be wired and plugged in to remotely mediated forms of communication and interaction. In one sense (excluding direct observation by police in public places) it is not homeless persons who are most subject to surveillance; rather it is the more privileged.

Indeed the very state of *being off the system*, which can partly define low or lumpen proletariat status, also brings with it a perverse kind of freedom to be left alone. Increasingly it is the more privileged *on the* *system* whose electronic transactions are subject to surveillance.

New styles of electronic living in some ways alter the traditional relationship between surveillance and stratification. For George Orwell it was not the masses but the elites who were most closely watched. As life comes to imitate art, contemporary electronic lifestyles reverse some aspects of the traditional relationship between stratification and surveillance, at least with respect to documentary records of behavior. The deep immersion of the more privileged in new documentary record forms of communication and interaction comes with some ironic vulnerability.

Excluding their greater pregnability to being observed in public places, in being unplugged, the poor and transitory homeless, are in some ways *less* subject to surveillance than the more privileged and located. Contrast the latter's telephone, fax, computer, bank, credit, employment, medical, and travel electronic trail- and tale-leaving behavior.

Awareness of the above factors modifies but does not overturn the stratification–privacy invasion link. Such awareness can help us see that indeed technology is a double-edged sword with respect to social stratification (and much else), even if its multiple blades are not of equivalent sharpness.

References

Brinn, D. (1999). *The Transparent Society*. New York: Perseus.

Coser, R. (1961). "Insulation from Observability and Types of Social Conformity," in *American Sociological Review* 26: 28–39.

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

Lace, S. (2005). *The Glass Consumer: Public Surveillance in a Surveillance Society*. Bristol: Polity Press.

Lyon, D. (2003). *Surveillance as Social Sorting*. London: Routledge.

Mann, S., Nolan, J. and Wellman, B. (2003). "Sousveillance: Inventing and Using Wearable Computing Devices for Data Collection in Surveillance Environments," in *Surveillance and Society* 1: 331–355.

McCahill, M. (2002). *The Surveillance Web*. Devon, U.K.: Wilan.

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