Secrecy and Society

ISSN: 2377-6188

Volume 1 | Number 1

Article 3

November 2016

Humpty Dumpty Was Wrong - Consistency in Meaning Matters: Some Definitions of Privacy, Publicity, Secrecy, and Other Family Members

Gary T. Marx
MIT

Humpty Dumpty Was Wrong - Consistency in Meaning Matters: Some Definitions of Privacy, Publicity, Secrecy, and Other Family Members

Keywords
definitions, privacy, secrecy, surveillance

Humpty Dumpty was Wrong - Consistency in Meaning Matters: Some Definitions of Privacy, Publicity, Secrecy and other Family Members[1]

Gary T. Marx

"When I use a word," Humpty Dumpty said in rather a scornful tone, "it means just what I choose it to mean — neither more nor less."

"The question is," said Alice, "whether you can make words mean so many different things."

"The question is," said Humpty Dumpty, "which is to be master – that's all."

- Lewis Carroll *Through the Looking Glass*

Humpty Dumpty was partially right. His words may mean what he chooses to have them mean, but that is just his story.[2] There is nothing inherent or eternal in the words (or what they represent). Granted that he has the power to say what *he* means, but others have the power to say what they mean, not to mention hearing what they choose to hear. Alice is the more interesting of the two when she wonders what the consequences are of making "words mean so many different things." For the understanding of secrecy and related phenomena those consequences are decidedly negative.

In the beginning there was the concept. And in beginning an inquiry into surveillance (Marx 2015), I argue that the failure to

adequately define and differentiate terms can cloud and contort ethical and empirical understanding and lead to unnecessary conflict and unwise policies. Consider surveillance and privacy, terms central to understanding secrecy. What "are" they really? (Or better what do people mean when they use the terms)?

In popular and academic dialogue surveillance is often wrongly seen to be only the opposite of privacy—the former is seen as bad and the latter good. For example, social psychologist Peter Kelvin (1973) emphasized privacy as a nullification mechanism for surveillance. But Kelvin's assertion needs to be seen as only one of four basic empirical connections between privacy and surveillance. Surveillance is not necessarily the dark side of the social dimension of privacy.[3] Surveillance implies an *agent* who *accesses* personal data (whether through discovery tools, rules, or physical and logistical settings). Privacy, in contrast, involves a *subject* who can *restrict access* to personal data through related means. But both can be connected in a variety of ways.

Surveillance can obviously invade privacy—that's what the fuss is all about (e.g., 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 (biometric identification and audit trails, video cameras that film those with access to sensitive

data). And privacy can also protect surveillance (undercover police who use fake IDs and call forwarding to protect their identity) just as it can nullify it (e.g., encryption, whispering, and disguises). Privacy for whom and surveillance of whom and by whom and for what reasons need to be specified.

Depending on how it is used, active surveillance can affect the presence of privacy and/or publicity. As nouns, the latter 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 to engage, find it optional to engage, or be prohibited from engaging in these activities, whether as subjects or agents of surveillance and communication

The rules applying to agents and subjects are in principle independent. 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, or that gives the subject discretion regarding revelation. Rather there is the

reverse—the subject has an obligation to reveal and/or the agent to discover.[4]

Private and Public as Adjectives

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

Of course, normative expectations of privacy and publicity do not always correspond to how the adjectives *public* and *private* are applied to empirical facts. Thus, the cell phone conversations of politicians and celebrities that have privacy protections may become public.

Information subjected to publicity requirements, such as government and corporate reports and disclosure statements, may be withheld, destroyed, or falsified. Information not entitled to privacy protections, such as child or spouse abuse, may be unknown because of the inaccessibility of the home to broader visibility. The distinction here calls for empirical analysis of the variation in the fit between the rules about information and what actually happens to it.

In consideration of the role of borders below, I note that privacy and publicity can be thought of in literal and metaphorical spatial terms involving invisibility and visibility and inaccessibility and accessibility. The privacy offered by a closed door or a wall and that offered by an encrypted e-mail message share information restriction, even as they differ in many other ways. Internet forums are not geographically localized but in their accessibility can be usefully thought of as public places, not unlike the traditional public square, where exchanges with others are possible or where others are visible, as with an uncovered window.

Those who make claims about privacy would be more likely to agree with one another, or at least be clearer in their arguments, if they clarified whether they were talking about respect for the rules protecting privacy or the empirical status of information as known or not known.

All concepts are of course limited, if not necessarily always scandalous. Erving Goffman (1971). In writing of "relations in public" and "public life," attends to the elements and possibilities within the immediacy of physical co-presence (that is in the presence of another person). This is the strand of "publicness" as visibility. It suggests the "public" as known to at least one other person rather than to any rules about the status of information (that it must be revealed or concealed) or to a legally defined place (such as private golf course). So he/we can paradoxically speak of "public order in private places" (Goffman 1971, xiv)

Such visceral immediacy sets up a nice comparative issue as a cousin of the distanced immediacy we have come to know—love and hate—through the Internet, cell phone, and webcam. It also alerts us to the neglected theme of private order and disorder (one form being privacy violations) in public places. Erving Goffman captures the former with his felicitous phrase *civil inattention.* For example, when passing another person we do not know on the street, some minimal glance is necessary in order not to collide and perhaps to acknowledge the other's presence. [5]The other is "available" for a more indelicate personal border crossing, but it does not occur. When it does occur, whether as a result of staring, leering or inappropriate speech, gestures or touch we have an instance of *uncivil attention* (Gardner

1995)

Confidentiality and Secrecy

Surveillance takes place in the context of rules, expectations, and practices regarding publicity and privacy. *Privacy* and *publicity* and *secrecy* and *confidentiality* are inherently social terms. The terms would be irrelevant to Robinson Crusoe when he thought he was alone on the island. They are social in implying an "other" from whom information is withheld or to whom it is communicated and who may, or may not, be under equivalent expectations to reveal and conceal. This section examines the interrelationships of rules regarding secrecy and confidentiality and helps clarify their meaning.

Confidentiality refers to rules about how discovered information is to be treated. It necessitates at least two parties and calls attention to social interaction and the rules and expectations that enshroud it. For confidentiality to be honored as a practical matter, a second party must have obtained the information. For example, once a doctor appropriately has personal information about a patient, the information is no longer "private" from the doctor. We can't speak of the doctor's invading the privacy of the patient through routine data collection (assuming other unrelated borders are honored). We can however speak of a violation of the rules of confidentiality if the doctor

wrongly shares the information or does not adequately protect it.

The information can be viewed as a shared secret, even though the prohibition on revelation (except under approved conditions) applies only to the surveillance agent (the doctor). This contrasts with settings where secrecy and revelation are reciprocal obligations, as with nondisclosure clauses in some contractual relations or court settlements.[6] When the interests of the parties overlap, the information is more likely to remain secret.[7]

Some analysts draw a distinction between secrecy and privacy. *Privacy* is used to mean shielding legitimate, non-stigmatizing information, while *secrecy* "implies the concealment of something which is negatively valued by the excluded audience and, in some instances, by the perpetrator as well" (Warren and Laslett 1977).[8] This definition of secrecy slaps a negative value on protected information. Such information may also be positively valued or neutral. A broader definition that does not start with the negative is needed.

To be sure, the nature and properties of any piece of information suggest an important set of variables. As noted, this discussion is particularly concerned with personal information, as against that about organizations or the physical world. The kind of information withheld by, revealed by, or taken from an individual is significant. Is it stigmatizing, morally disvalued, disadvantageous; morally and socially

neutral; or prestige enhancing, morally valued, and advantageous? The organization and dynamics of information control (whether to discover or communicate/publicize information or to block these) of course will differ depending on the kind of information.

The motives and related goals for protecting, discovering, and communicating personal information are certainly important. Thus, it is useful to differentiate information that others do not know according to the degree of intentionality found with the withholding and the relative importance the individual places on controlling the information. When the non-revelation of the secret is associated with "something to hide" (either as stigma or non-stigmatizing information that would disadvantage), we see greater intentionality than in situations where the unavailability or withholding of information flows from a sense of propriety or natural conditions such as limits on the senses.

By convention, the term *secrecy* often refers to organizational data, while *privacy* refers to the data of individuals. Since organizations do not generally have "rights" in the same sense that individuals do, *secrecy* is a better term here than *privacy*. This may involve *legitimate organizational secrets,* as with patent details and strategic plans, or *illegitimate organizational secrets,* as with false reporting and cover-ups. The rules around organizational information, as with those around personal information, vary from mandatory

disclosures to closures with a large discretionary middle area. [9]

However, apart from legal meanings, many of the information-control processes are the same regardless of whether we are dealing with organizations or individuals. What is fundamental is the issue of information control. There is no compelling reason to call the protection of negative information secrecy and its opposite privacy. Whether as noun, adjective, or verb, the meanings of *secret* and *secrecy* overlap those of *privacy* and *private*. When personal privacy is viewed as a right, it calls attention to the subject's ability to control the release of information. This does not mean it cannot be shared, but that the individual has a choice. The Fifth Amendment, for example, does not prohibit individuals from offering information or confessing, it simply prohibits this from being coercively obtained.

In contrast, the rules applying to legitimate secrecy prohibit or limit the subject from releasing information. This is often accompanied by sanctions for violation. In principle, individuals and organizations don't have a choice about divulging information deemed to be secret by formal rules. Thus, the broader terms *protected* and *unprotected information* can be used to include both privacy and secrecy and their opposites,[10] whether this refers to the rules about the information or its current empirical status.

Types of Privacy

Privacy, like the weather, is much discussed, little understood, and not easy to control. Like its family member *surveillance,* it is a multidimensional concept with fluid and often ill-defined, contested, and negotiated contours, dependent on the context and culture. The scholarly effort to define privacy is a growth industry. Yet as welcome as deductive conceptual efforts regarding the meaning of privacy are, they must be approached deftly lest they end in reification and nominalism gone wild. I prefer to begin with empirical topics that are intellectually and socially compelling and to inductively generate concepts from them.

For our purposes, the central factors are the rules and conditions affecting data outputs from and inputs to the person. These rules and conditions encounter and may create or overcome borders around the person—whether natural or cultural. As noted, I use the term *data* or *information* to broadly refer to various sensory phenomena that may cross the borders of the person (whether leaving or entering) or otherwise be associated with the person.

Contemporary concerns almost always involve some aspect of informational privacy, a form early identified by Westin (1967). I don't wish to enter the debate over what privacy "really" is in some essentialist pre-social sense. But I will note how a sociology-of-information approach connects to themes in the literature. 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 borders are obviously more difficult to cross if an individual cannot be reached via name or location. The conditions around revelation or protection of various aspects of identity are central to our topic.

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.[11]

A related and taken-for-granted form is aesthetic privacy (Rule et al, 1983), which refers to the separation, usually by a physical barrier of bedroom or bathroom, of activities involving one's "private parts" and unguarded moments. Alderman and Kennedy (1995) discuss a number of such cases in which the shock of discovering a violation surfaces norms of which we are hardly aware because they are so rarely violated. Clothes and manners also sustain aesthetic privacy. The concern over full-body airport scans also illustrates a violation or breach of such norms.

Informational privacy can be considered as it ties to institutional setting (e.g., financial, educational, health, welfare, employment, criminal justice, national security, voting, census); places and times; the kind of data involved, such as about religion or health, apart from the setting; participant roles (communications privacy as involving two-party, one-party, or no-party consent); and aspects of technology, such as wire or wireless, phone, computer, radio, or TV. Considerations of setting, data type, and means are central to legislation and regulation and rich in anomalies and cross-cultural differences.

In emphasizing informational privacy, several other commonly considered forms such as decisional (Decew 1997) or proprietary (Allen 2007) privacy are slighted.[12] Breaches of these forms primarily involve application or use of private information, rather than information discovery. Although it is 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. These may be 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—then they need not worry about that information's being used.

Borders

When you are heading for the border Lord
You're bound to cross the line.

- Kris Kristofferson, "Border Lord"

Much of human history can be read as a struggle involving the access to and symbolism implied by various kinds of spatial and metaphorical borders. The intersection and blurring of the borders of personal information and technology under conditions of modernization and globalization are central to the topic.[13] When surveillance and communication technology are controversial, it is often because of the crossing, or the failure to cross, a personal border, or because border definitions conflict.

Various borders may protect information: physical blockages such as walls, a purse, or skin; kinds of places or organizations as culturally defined, such as a home, a church, or a public park; kinds of role relationships, such as professional and familial; and various temporal forms, such as time after working hours, leisure time, holidays, and amnesty periods.

Various images can be applied. We can think of borders around the person as being like a bubble, clear, frosted, or opaque and hermetically sealed or permeable—and for the last, whether permitting outputs, inputs, or both. With the piercing abilities of the new surveillance, speaking of the *borderless person* (or even organization

or nation may become less of an oxymoron.

The idea of borders suggests a circumscribed entity (in this case, the person) separate from its environment. Yet borders to varying degrees permit exchanges or, as they say, "flows." This quality alerts us to the important and neglected issue regarding the directionality of border crossings. Borders, like roads, are navigable in several directions.

Technologies that cross personal borders can be differentiated based on the direction of the crossing and data flow. These issues tie to sociology-of-information questions regarding norms about concealing and revealing information. Here violations may occur on the part of both the surveillance agent and the person of interest, in either failing to collect or offer information. An example of the former would be an agent's failure to collect vital information from expectant mothers such as about drug use (Etzioni 1999) or inquiring about arrest history for persons working with children. Examples of the latter would be a subject's failure to reveal such as a house seller concealing a leaky roof or a person with a sexually transmitted disease not informing a partner of this. Most academics and activists emphasize the involuntary collecting of personal information by agents while generally giving little attention to the failure to surveil or of subjects to `fess up.

However, considerations of privacy need to focus on more than only taking from the person or failing to do so or the failure to reveal. Crossing a personal border to impose upon the person is of equal importance in considerations of liberty and in the generation of a broad and logical conceptual framework. Consider, for example, smells sent through a heating or air-conditioning system intended to affect moods or telephone solicitations, spam and regular junk mail or the bombarding of messages in some supermarkets over the PA system or written on the floor, shopping carts, and neon signs. Or consider individuals who offer information inappropriately, as with public nudity, loud music, or revelation of intimate life details to strangers.

Surveillance and Communication

The function of borders as either containing those within or rejecting those outside (or both) is being changed by new surveillance and communication technologies. The spread of sensors and their weaving into data networks especially calls attention to the connections between undifferentiated and differentiated forms of communication and surveillance. These technologies may be mass or individually based and involve extraction or imposition functions.

In most considerations of individual privacy, the emphasis is on the extent to which the individual can, in principle and in actuality, control data from flowing outward, such as that involving telephone or

computer communication, credit card activity, social networks, beliefs and feelings, location, facial appearance, or biometric data such as DNA, voice print, heat, and scent. When such outputs are available, the individual is a transmitter of data, and something is taken from or willingly leaves the person.[14] This transmission may happen in an active or passive fashion and with or without the individual's knowledge and consent.

Much less attention is directed to the individual's control over information and stimuli flowing inward, such as sound, sight, smell, touch, taste, and factors affecting the ability to act (the hard engineering in or out of behavior potentials) and even "cookies" placed on one's computer by web sites visited. Here the individual is a potential recipient of information and related inputs, opportunities, and restrictions from outside. These in a sense enter rather than leave the person, or at least the person's environment.[15]

While we are often happy magnets for such exterior inputs, much energy also goes into constructing and sustaining barriers to unwanted communication forms, such as advertisements (the TV mute button, DVR), spam, telemarketing, and junk mail ("do not contact" lists, call restriction devices), outside noise (headsets), and wearing hats, dark glasses, and even masks in public. Such inputs also extend to the unwanted communication from loud cell phone users in public

places. In such cases we see the desire to be left alone and for "space" and distance, or at least insulation from others.

The same technology may of course offer outputs and inputs.[16] What surveillance takes from the individual can be joined with a reverse flow of communication imposed upon the individual. The telescreeen in George Orwell's novel *1984* illustrates this. It transmitted the person's image and words to Big Brother, while simultaneously broadcasting propaganda.

Foucault (1977) observed the move away from the spectacle of irregular public executions as control mechanisms intended to instill fear in the audience to softer punishment hidden and controlled within institutions. The systematic use of supposedly scientific knowledge and less visible surveillance were thought to be more effective and humane. Yet with developments in mass communication and the strengthening of the First Amendment, public access to information is strong and may be getting stronger. We see not only the few watching the many, but the many watching the few, sharing the same logic of visibility intended to bring deterrence and accountability. The news entertains and also brings morality tales and symbolic meanings (Altheide 2002; Andrejevic 2007; Doyle 2003; Leman-Langlois 2002; Mathiesen 1997). Entertainment in the form of sitcoms, music videos, and video games brings the news and morality tales.

In the year 1984, Jim Rule observed that with the development of computing, mass surveillance became possible alongside mass communication. In its indiscriminate sweep, the mass surveillance of generalized computer matching (in which the two or more entire databases are compared absent reason for specific suspicion) is equivalent to the indiscriminate mass transmission of a TV or radio signal.

Beyond being mass (broadly) directed, as with TV ads or video cameras on roads, communication and surveillance may be focused with varying degrees of specificity on individual subjects of interest, as with targeted marketing and court-ordered wiretaps. This distinction (mass or individual focus) is considered in Chapter 2 of my book *Window Into the Soul* mentioned above.. Here let us simply note some links and some blurring between the two.

We increasingly see tools such as video and computer technologies that combine surveillance and communication functions or blur the line between them. With this comes a move from mass to more individualized communication determined by characteristics of the recipient. Moreover, developments in the surveillance of consumption have been a major boost to targeted forms of communication.

Individualized (targeted or segmented) marketing

communication often occurs as a result of some form of surveillance. Calls to an 800 number, visits to a web page, or consumption behavior can lead to spam or targeted solicitations via telephone and mail. Law enforcement also uses mass communications such as advertisements and mailed solicitations to identify potential offenders (those who respond), who may then become subjects of stings and other forms of surveillance.

Contemporary television and webcam transmissions also combine or blur the line between surveillance and communication. Consider live helicopter videos of car chases, as with O. J. Simpson, or investigative TV programs that use infiltration and stings to uncover consumer fraud and sexual predation. In these cases, the surveillance function is seen as a means for the collection of evidence, as an aide to apprehension of violators, and as an affirmation of cultural beliefs about what happens to them. This line blurring is also seen with home cable TV systems that beyond offering entertainment can monitor viewer behavior for billing, marketing, and security. In the case of the latter they can monitor for fire, gases, functioning of electrical and other systems, unauthorized entry or motion, and internal images of the home when an alarm is triggered.

The same tool of course may serve different functions for various groups. Webcam transmissions such as those in bars or on beaches

that offer images of swimmers and weather conditions also serve as means of communication and control. Automobile radios deliver music and emergency messages (the latter even if the radio is turned off), and electronic location and engine monitoring devices can control driving behavior while also offering safety warnings. Multifunction handheld devices that offer radio and television can receive and transmit personal messages and images, while also offering records of location and communication usage.

In summary, communication and surveillance may be mass (broadly) directed, as with TV ads and video cameras in a public square. Or they may be individually focused with varying degrees of specificity on subjects of interest, as with marketing to particular demographic groups and air travel profiling. Technical and social developments have strengthened both forms, the linkages between them, and their merging.

Greater attention to the non-self evident meaning of the common sense terms this article has discussed hardly guarantees wise public policies with respect to the information control issues so central to a democratic society, but it is surely a necessary condition.

References

Altheide, David. 2002. *Creating Fear: News and the Construction of Crisis.* Hawthorne, NY: Aldine de Gruyter.

_____. 2006. *Terrorism and the Politics of Fear.* Lanham, MD: AltaMira Press.

Andrejevic, Mark. 2007. *iSpy: Surveillance and Power in the Interactive Era.* Lawrence: University of Kansas Press.

Alderman, Ellen, and Caroline Kennedy. 1995. *The Right to Privacy.* New York: Knopf.

Allen, Anita L. 2003. *Why Privacy isn't Everything: Feminist Reflections on Personal Accountability.* New York: Rowman and Littlefield.

Coll, Sami. 2012. "The Social Dynamics of Secrecy: Rethinking Information and Privacy through Georg Simmel." *International Review of Information Ethics* 17 (7), 15-20.

Decew, Judith W. 1997. *In Pursuit Of Privacy: Law, Ethics, and the Rise Of Technology.* Ithaca, NY: Cornell University Press.

Doyle, Aaron. 2003. *Arresting Images: Crime and Policing in Front of the Television Camera.* Toronto: University of Toronto Press.

Etzioni, Amitai. 1999. *The Limits of Privacy.* New York: Basic Books.

Foucault, Michel. 1977. *Discipline and Punish: The Birth of the Prison.* New York: Pantheon Books.

Goffman, Erving. 1971. *Relations in Public.* New York: Basic Books.

Kelvin, Peter. 1973. "A Social-Psychological Examination of Privacy." *British Journal of Clinical Psychology* 12(3), 248-261.

Koops, Bert-Jaap, Newell, Bryce Clayton, Timan, Tjerk, Škorvánek, Ivan, Chokrevski, Tom, and Galič, Maša. 2016. "A Typology of Privacy." *University of Pennsylvania Journal of International Law,* 38(2) forthcoming. http://scholarship.law.upenn.edu/jil/

Leman-Langlois, Stephane. 2008. *Technocrime: Technology, Crime, and Social Control.* Devon, UK: Willan Publishing.

Marx, Gary T. 2016a. "Genies: Bottled and Unbottled: Some Thoughts on the Properties of Information." In M. Hildebrandt and B. van den Berg, *Freedom and Property of Information: The Philosophy of Law Meets the Philosophy of Technology,* 10-33. New York: Routledge.

_____ . 2016b. *Windows into the Soul: Surveillance and Society in the Age of High Technology*. Chicago: University of Chicago Press.

_____. 2015. "Coming to Terms: The Kaleidoscope of Privacy and Surveillance." In *Social Dimensions of Privacy: Interdisciplinary Perspective*, edited by Beate Roessler and Dorota Mokrosinska, 32-49. Cambridge: Cambridge University Press.

_____. 2011. "Turtles, Firewalls, Scarlet Letters and Vacuum Cleaners: Rules about Personal Information." In *Privacy in America: Interdisciplinary Perspectives*, edited by William Aspray and Philip Doty, 271-294. Lanham, MD: Scarecrow Press.

Marx, Gary T., and Glenn W. Muschert. 2007. "Personal Information, Borders, and the New Surveillance Studies." *Annual Review of Law and Social Science* 3, 375-395.

Mathiesen, Thomas. 1997. "The Viewer Society: Michel Foucault's 'Panopticon' Revisited." *Theoretical Criminology* 1(2): 215-234.

Packard, Vance O. 1957. *The Hidden Persuaders.* New York: Pocket Books.

_____. 1964. *The Naked Society.* New York: Penguin Books.

Rule, James B., Douglas McAdam, Linda Stearns, and David Uglow. 1983. "Documentary Identification and Mass Surveillance in the United States." *Social Problems* 31(2): 222-234.

Scheppele, Kim Lane. 1988. *Legal Secrets: Equality and Efficiency in the Common Law.* Chicago: University of Chicago Press.

Simmel, Georg. 1950. *The Sociology of Georg Simmel.* Edited by Kurt H. Wolff. New York: Free Press.

Turrow, Joseph. 2012.*The Daily You How the New Advertising Industry is Defining Your Identity and Your World.* New Haven: Yale University Press.

Warren, Carol, and Barbara Laslett. 1977. "Privacy And Secrecy: A Conceptual Comparison." *Journal of: Social Issues* 33 (3):43-51.

Westin, Alan F. 1967. *Privacy and Freedom.* New York: Athenum.

[1] This article draws from Marx, *Windows into the Soul: Surveillance and Society in an Age of High Technology* (2016c) and other works (2015; 2016a; 2016b).

[2] With apologies to the immortal lines of the Dude in the film *The Big Lebowski* "that's just like, your opinion, man."

[3] The noun *surveillance* and the verb *to surveil* are the same figures of speech as *privacy* and *to privatize*. The latter, however, have their opposites in *publicity* and *to publicize*. But where are the equivalent opposites for *surveillance* as a noun and a verb? In English there is no easy term for the action which is the opposite of surveillance. The verb form *to surveil* suggests actively surveying by an agent, just as the verb form *to privatize* suggests actively protecting (although the more common usage involves property rights, as with privatization). While *publicize* is the opposite of *privatize*, the best-worst term we have for a potential surveillance agent who doesn't act is that he or she demonstrates anti- or non-surveillance or perhaps un-observance. The agent chooses not to act or to know (as with the proverbial three monkeys).

[4] Marx (2011) analyzes the four types.

[5] However sometimes the inattention is feigned as with the so-called *brush pass* in which two people who appear to be simply brushing past each other are handing off spy material in the best tradecraft tradition.

[6] Contrast this with various other patterns, such as those of non-confidentiality, where both can or must reveal, or where the surveillance subject also is expected not to reveal. The presence or absence of reciprocity and prohibitions or prescriptions on discovering and reporting are important variables in structuring and judging surveillance settings.

[7] This suggests another typology of not only who the rules apply to, but of whether the interests of the parties to the secret are shared or conflicting. Consider the secrecy sustaining elements of those having affairs, involved in conspiracies, and the reluctant symbiosis of players in the game of blackmail, as against situations where the parties have non-overlapping interests in revelation and concealment.

[8] For this view we can blame Georg Simmel: "The secret is . . . the sociological expression of moral madness" (1950, 331). While Simmel is the classical theorist I would most like to meet if had I to write about that for an SAT essay test, he missed it here. Marx and Muschert (2008) and Coll (2012) argue for Simmel's continuing relevance a century later, particularly with respect to secrecy and information control, new forms of sociation and information as a new medium of exchange.

[9] Scheppele (1988) offers a useful conceptualization in noting secrets may be direct (*A* withholds from *B*), serial (*A* shares the secret with *B* but withholds it from *C*) or collective (*A* and *B* create a secret that they jointly withhold from *C*). For these three structures there are two choices -- to tell or not to tell. This leads to six types of secret based on the parties involved and whether the information is revealed or concealed ((disclosure, betrayal, leaks, simple secrets, secondhand secrets, and conspiracy). A further distinction involves whether or not the target of the secret suspects that there might be a secret. In that case we find *shallow secrets. Deep secrets* refer to cases where the subject does not imagine that relevant information might be had. Making such distinctions can improve the asking of research questions and judging the morality of information concealing and revealing.

[10] For the word *private* the opposite is *public* but what is it for *secret* (*non-secret*) and what does the lack of an equivalent term imply?

[11] The physical border perspective has limits too, thus taking or giving a urine or breath sample or a photo involves using things that have already left the body and are different and beyond the literal physical protective border of it. Garbage placed on the street in a protective container is physically (although not impossibly) bordered as well, and in some jurisdictions is also legally bordered.

[12] Defining cases such as *Griswold v. Connecticut*, 381 U.S. 479 (1965), and *Roe v. Wade*, 410 U.S. 11 (1973), involve decisional privacy with respect to personal and intimate matters such as family planning, birth control, same-sex marriages, or physician-assisted suicide. Proprietary privacy—use of a person's information without consent for commercial and other purposes—also involves control and liberty questions and the extension of market principles to symbolic material that is often immaterial (at least physically). Drawing on, but going beyond these

types, Jaap *et al* offers a comparative analysis of privacy that combines the two variables (constitutional principles involving freedom from and freedom to and behavioral zones involving the personal and the public to yield eight basic types of privacy (bodily, intellectual, spatial, decisional, communicational, associational, proprietary, and behavioral privacy), with an overlay of a ninth type (informational privacy) overlapping but not coinciding the others. Available at: http://ssrn.com/abstract=2754043

[13] In Marx (1997, 2001, and 2005b) some blurred forms considered are space, distance, darkness, time, and social and cultural orders.

[14] The largest category is probably residual, in which there are no rules (although there may be softer expectations). What is the ratio of rules that prohibit revelation, as with public nudity or nursing, to those that mandate revelation, as with the obligation of sellers of a car or home to come clean, and what are the ratios for prohibiting or requiring asking for information?

[15] These distinctions can get hazy and be sequentially linked. Consider implants which enter the person but can then send data back from the person under external or internal triggering as with an RFID chip or bombarding a person with stimuli and then "reading" the response, as with one of the MRI brain techniques.

[16] Vance Packard was prescient here in writing about both taking information from and imposing it upon the individual, although the dates (1964 and 1957) of his publications reverse this logical sequence. Goals do not seem to have changed, even as the tools have changed.