Reason and Insight

Western and Eastern Perspectives on the Pursuit of Moral Wisdom

SECOND EDITION

Timothy Shanahan
Loyola Marymount University

Robin Wang
Loyola Marymount University

THOMSON
WADSWORTH

Australia • Canada • Mexico • Singapore • Spain • United Kingdom • United States

Publisher: Holly J. Allen
Philosophy Editor: Steve Wainwright
Assistant Editor: Lee McCracken
Editorial Assistant: Anna Lustig
Technology Project Manager: Susan DeVanna
Marketing Manager: Worth Hawes
Marketing Assistant: Justine Ferguson
Advertising Project Manager: Bryan Vann

Printed in Canada

1 2 3 4 5 6 7 06 05 04 03 02

For more information about our products, contact us at:

Thomson Learning Academic Resource Center
1-800-423-0563

For permission to use material from this text, contact us by:

Phone: 1-800-730-2214
Fax: 1-800-730-2215
Web: http://www.thomsonrights.com

Library of Congress Control Number: 2002104238

ISBN 0-534-50599-6

Print/Media Buyer: Barbara Britton
Permissions Editor: Charles Hodgkins
Production Service: Scratchgravel Publishing Services
Copy Editor: Toni Ackley
Cover Designer: Ross Carron
Printer: Transcontinental Printing
Compositor: Scratchgravel Publishing Services

Wadsworth/Thomson Learning
10 Davis Drive
Belmont, CA 94002-3098
USA

Asia
Thomson Learning
60 Albert Street, #15-01
Albert Complex
Singapore 189969

Australia
Nelson Thomson Learning
102 Dodds Street
South Melbourne, Victoria 3205
Australia

Canada
Nelson Thomson Learning
1120 Birchmount Road
Toronto, Ontario M1K 5G4
Canada

Europe/Middle East/Africa
Thomson Learning
Berkshire House
168-173 High Holborn
London WC1V 7AA
United Kingdom

Latin America
Thomson Learning
Seneca, 53
Colonia Polanco
11560 Mexico D.F.
Mexico

Spain
Paraninfo Thomson Learning
Calle/Magallanes, 25
28015 Madrid, Spain

enhance security for its citizens, how much freedom should be given to the government to monitor phone lines, to access private email messages, to require that every citizen carry and display a government-issued identification card, and to employ other forms of surveillance in order to monitor their activities? Such questions have no easy answers. But it is critical that such questions be raised, and that the answers arrived at be subjected to careful examination.

Reading Questions

1. According to DeCaroli, how have technological innovations begun to "destablize" our conception of privacy? How have methods of gathering personal information through the use of computer technology begun to blur the distinction between what is "public" and what is "private"?
2. Why does DeCaroli believe that there is a (at least potential) dilemma between the desire to live in a society in which personal privacy is guaranteed, and to live in a society safe from criminal activity? What specific example(s) does he use to illustrate this claim?
3. DeCaroli notes that "security is always a matter of access." What does he mean by this? What sorts of problems are generated by the desire to make something (e.g., personal information) both secure and accessible?
4. What does DeCaroli mean by "forged membership"? Why does he believe that "many, if not most, security threats . . . can productively be understood as a form of forged membership"?

Assuming Identities: Media, Security, and Personal Privacy

STEVEN DECAROLI

I

A central organizing principle of Western political thought since classical antiquity has been the distinction between the public and the private. As far back as the Homeric epics, the Greek language has recognized a basic distinction between those activities of an individual performed for personal reasons and those actions undertaken by an individual in the service of a public office. When, in the *Odyssey*, Menelaus asks Telemachus if his quest is done for public or private reasons (*demion e idion*) Homer is making just such a distinction.[1] Here the Greek *idios* refers specifically to that which is "one's own," to that which "pertains to one's self," while the word for public, *demios*, denotes that "having to do with the people [as a whole]."[2]

While there is much in the Greek terminology that overlaps with our modern usage of the terms public and private, it would be a mistake to assume that the meaning attributed to the terms of this dichotomy have remained stable. As Barrington Moore has shown, the use of the term for that which is private, *idios*, did not carry for the ancient Greeks the positive overtones that it would acquire, for instance, in the political writings of the Natural Law theorists of the seventeenth century.[3] In fact, evidence of the negative

[1]Homer, *Odyssey*, 4.314.

[2]Liddell and Scott, *Greek-English Lexicon* (Oxford: Oxford University Press, 1977).

[3]Barrington Moore, Jr., *Privacy: Studies in Social and Cultural History* (London: M. E. Sharpe, 1984), 82.

Steven DeCaroli, "Assuming Identities: Media, Security, and Personal Privacy." Reprinted by permission of the author.

connotation that *idios* had for the ancient Greeks can be observed in the etymological history of its noun form, *idiotes*, which comprises the root of the English derogative, *idiot*. For the Greeks, private life was a derogatory designation directly associated with the laborer, the layman, and with those who did not hold public office and could not, therefore, participate in the political life of the *polis*. Today, however, in the United States at least, it is public life, that is to say, political life and its institutions, that often are considered a threat to private life insofar as actions taken on behalf of public interests are very often interpreted as encroachments into private matters.

The values attributed to the public and the private are, therefore, contingent upon the specific context in which they appear. Attempts to determine *a priori* the values associated with the private or the public are bound to fail, not only because the respective virtues of private life and public life vary greatly from culture to culture and epoch to epoch, but also because the specific content associated with each of these social jurisdictions cannot be abstractly determined. The most one can say is that, at a basic level, the private and the public are reciprocally determined concepts—in other words, that which is not considered to be public is, by and large, deemed to be private and that which is not private is considered public. Consequently, the content appropriate to the public and the private varies greatly from one community to another, for almost anything one can think of can be considered, at one time or another, or in one possible community or another, a matter of privacy or publicity. Those aspects of life that the modern West deem to be most private, bathing and defecation, for instance, were regularly performed in public in ancient Rome, often in the open air and visible to all. To simply say that in adopting these practices the Romans did not recognize privacy would clearly be mistaken. The point is simply that privacy does not correspond to a fixed content, but rather is the outcome of customs specific to individual communities. While life in all political communities is characterized by members who simultaneously inhabit public and private social jurisdictions, the explicit content of these jurisdictions, and particularly that of the latter, remains impossible to specify in the abstract.

Given that the value and meaning of privacy have undergone dramatic changes throughout Western history, it is worth considering how, and to what extent, current transformations in modern society continue to affect our basic understanding of privacy, and to estimate how this understanding influences the ethical and legal claims we make regarding it. But before discussing the contemporary relevance of privacy, or more specifically, before examining how technological innovations in data accumulation and filtering, coupled with the influence of rapid and pervasive media coverage, have begun to destabilize our conception of the term, it is important to first examine the modern genealogy of the concept so as to illustrate how privacy, in conjunction with its reciprocal concept, publicity, came to play a central role in the formation of modern liberalism. It is only after one has a clear sense of how the concept of privacy has been used in recent times that one can accurately identify the ways in which it is currently being altered.

Following a discussion of how modern liberalism established formal conditions for thinking about privacy, particularly through efforts to secure the safety of persons and property, I will consider how modern methods of gathering personal information through the use of computer technology have begun to blur the line between what is public and what is private. In the process, particular attention will be paid to issues raised by, on the one hand, the widespread desire to live in a society where robust individual privacy is guaranteed, and on the other hand, the equally common aspiration to live in a society safe from criminal (i.e., intentionally harmful) activity of all types. The dilemma that lies at the heart of these two demands arises from the fact that, in order to maintain the conditions necessary to fulfill the second demand, the goals of the first demand must be compromised. Creating a secure society requires, at some level, the use of surveillance not only to observe actions, but more essentially, to identify and keep track of individuals who perform these actions. The very means by which individuals are monitored, however—be it through security cameras and tax audits, or through the apparently more benign practices of issuing driver's licenses, passports, and even birth certificates—are precisely the means whereby individual privacy is intruded upon. In determining how much information ought to be gathered about individuals within a society, one is forced to weigh the harm, or potential harm, done by gathering such data against the harm prevented by gaining information which might assist in preventing certain harmful activities from occurring.

Due, however, to the exponential advancement and development of new technological means of surveillance and information analysis, it is becoming less and less clear where private life ends and where public life begins—particularly because marketing agencies, credit companies, commodity retailers, as well as the private media have, in numerous respects,

surpassed the state in monitoring and analyzing our behaviors. With the appearance of ever more efficient means of gathering and processing information not only has it become less clear exactly how much personal information is actually being accumulated about us in the course of our regular, day-to-day activities, but non-governmental organizations are increasingly able to compete with the state in gathering together publicly available information into vast repositories of raw data. By sorting through this daunting amount of information with the assistance of sophisticated software, non-governmental organizations are able to extract greater and greater levels of informational value, or "resolution," about our lives from data which only a few decades ago would have been dismissed as random and meaningless. Since virtually every aspect of economic and social life in the United States generates a record, and is therefore subject to inclusion in an informational database, it is incumbent upon us to reassess the so-called "right to privacy" in terms of a number of difficult and increasingly urgent questions: Who has the right to access personal information? To what purposes ought this information be applied? Under what conditions does private information become public? Is personal information a type of property? And if so, how does one claim legitimate ownership? And finally, what level of risk, and *inconvenience*, are we willing to assume for the sake of maintaining our personal privacy?

II

In her essay, "Humankind as a System: Private and Public Agency at the Origins of Modern Liberalism,"[4] Daniela Gobetti explains how the modern concepts of the private and the public find their roots in the work of early modern Natural Law theorists who were the first both to formulate a conception of the "citizen" as the bearer of legal power, and to use the notion of harm, or injury, as a key criterion for distinguishing between the public and the private. According to Gobetti, Natural Law theorists employed a notion of injury derived from Roman law "to convey the idea that the violation of what belongs to a person according to the law of nature constitutes harm."[5] Consequently, the social jurisdiction encompassed by the private sphere, conceived according to this principle of harm, includes all activities and possessions of an adult person which do not harm or threaten the safety of other private individuals. The social jurisdiction of the public sphere, on the other hand, while it overlaps with that of the private sphere in those instances where harm has taken place, is understood as being *in the service of* privacy. In other words, the public sphere corresponds to that collectively maintained authority which has the right to legitimately intrude upon a person's private jurisdiction either for the sake of preventing harm or to punish an injury already committed. It is, of course, government, acting in its capacity as an enforcer of common interests, that assumes this public role and regularly intrudes upon personal privacy. Ideally, governments should compromise individual privacy only as a way of ensuring the safety and well-being of private individuals and to ensure that these individuals retain the ability to act out private interests without unwarranted obstruction. In fact, it is precisely this limitation, applied to all governmental intrusions into private jurisdiction, that is expressed in Justice Louis Brandeis' consequential 1928 dissenting argument in *Olmstead v. U.S.* Here Brandeis asserts that, "they [the founders of the Constitution] conferred, as against the government, the right to be let alone—the most comprehensive of rights, the right most valued by civilized man. To protect that right, every *unjustifiable intrusion* by the government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the fourth amendment."[6]

Of all the early contract theorists whose ideas comprise the foundation of modern liberalism, it was John Locke who first explicitly employed the concept of injury as a means of gauging the distinction between public and private jurisdictions. In *A Letter Concerning Toleration*, Locke states the case quite clearly. "The part of the Magistrate," he writes, "is only to take care that the Commonwealth receive no prejudice, and that there be no Injury done to any man, either in Life or Estate."[7] For Locke, the legiti-

[4]Daniela Gobetti, "Humankind as a System: Private and Public Agency at the Origins of Modern Liberalism," in *Public and Private in Thought and Practice: Perspectives on a Grand Dichotomy*, ed. Jeff Weintraub and Krishan Kumar (Chicago: University of Chicago Press, 1997), 103–132.

[5]Gobetti, "Humankind as a System," 103.

[6]*Olmstead v. U.S.*, 277 U.S. 438, 478 (1928) (Brandeis, J. dissenting). Quoted in Alexander Rosenberg, "Privacy as a Matter of Taste and Right," in *The Right to Privacy*, ed. Ellen Frankel Paul, Fred D. Miller, Jr. and Jeffrey Paul (Cambridge: Cambridge University Press, 2000), 84. Emphasis added.

[7]John Locke, *A Letter Concerning Toleration*, ed. J. Tully (Indianapolis: Hackett Publishing, 1983), 42. Quoted in Gobetti, "Humankind as a System," 103.

mate right to own property is *the* fundamental characteristic of private life, and it was to insure that the right to own property remained unbroken that the public institution of a government was established. For according to Locke, objects are bound to one in the form of property, not through nature or through God's will, but through one's own labor which is expended in the act of making something. As he famously writes in the *Second Treatise of Government*, "Whatsoever then he removes out of the state that nature hath provided, and left it in, he hath mixed his *labour* with, and joined to it something that is his own, and thereby makes it his *property*."[8] Property, Locke contends, is the consequence of an annexation of oneself, in the form of one's labor, to an object during the process of its creation. Through this activity one removes an object from that assembly of things which, by nature, are common to all people, and places it among those things which are considered private. Consequently, any uninvited attempt on the part of another person to lay claim to that which is legitimately constituted as private property is, for Locke, tantamount to a threat on one's own body. Since it is a person's labor which legitimates ownership, and because labor is the irreducible product of a person's inalienable body, the bonds that tie property to individuals are the same as those which bind bodies to the individuals whose lives reside within them. Defensive actions against such threats are, therefore, as legitimate as an individual's right to protect his or her own body from harm.

The right to protect one's body is, therefore, a basic principle of privacy, and its most profound expression in Western political thought actually appeared a generation before Locke in the writings of Thomas Hobbes who, in his *Leviathan*, spoke of what he called the "right of nature." At the beginning of Book XIV of *Leviathan*, Hobbes defines the right of nature, or *jus naturale*, as simply, "the liberty each man hath to use his own power, as he will himself, for the preservation of his own nature, that is to say, of his own life."[9] Once again, it is a universal threat—in this case, posed by those individuals who, in exercising their own right to survival, may willingly harm those around them—which brings about the need to form a government, that is to say, the need to construct a public body whose purpose it is to secure the safety of private bodies and their property.

What is important to recognize in all of this is that the formulation of modern political theory in the West is premised on the need to institutionalize a relationship between the public and the private, and more specifically, that this relationship is fundamentally one of *security*. The hypothetical decision on the part of those individuals living in Hobbes' fictional "state of nature" to relinquish a portion of their natural rights, namely, their right to do whatever they wish to serve their own interests, is strictly motivated by the fear that they may lose their lives. What the state of nature cannot provide to the completely autonomous individual is the security necessary to act freely without undue fear of harm. The apparent paradox at the root of political authority is that one must sacrifice a degree of autonomy in order to save it. The contractual decision on the part of sovereign individuals to willfully reduce their autonomy for the sake of safety neatly illustrates the abiding connection that exists between security and privacy. Autonomy, which is generally conceded to be intimately associated with privacy,[10] must remain hindered, at least to a degree, if a viable state of security is to be established. The establishment of a secure society requires that utterly sovereign individuals submit themselves to the authority of a sovereign whose power will be exercised in public—a sovereign whose very reason for being is a constant, though often innocuous, infringement on the private lives of individuals for the sake of greater security.

To the extent that this is true, the condition for the possibility of security for Hobbes is the institution of a form of *membership* which is entered into when individuals agree to certain common interests. The customary name given to this political agreement is, of course, the "social contract." In order to be a recipient of the security promised by Hobbes' political organization, individuals must join, through a contractual obligation, a group of other individuals who will, at the very least, hold one accountable for the terms of that contract. And it is precisely the enforcement of these obligations through a publicly exercised system of accountability in the form of a sovereign power that permits a state of security to prevail. Indeed, I will go so far as to say that, though often not immediately recognizable, *all forms of security involve some form of membership*, be they voluntary or involuntary, extensive or limited. And in each case, membership is

[8]John Locke, *Second Treatise of Government*, ed. C. B. Macpherson (Indianapolis: Hackett Publishing, 1980), 19.
[9]Thomas Hobbes, *Leviathan*, ed. Edwin Curley (Indianapolis: Hackett Publishing, 1994), 79.

[10]See Lloyd L. Weinreb, "The Right to Privacy," in *The Right to Privacy*, ed. Ellen Frankel Paul, Fred D. Miller, Jr. and Jeffrey Paul (Cambridge: Cambridge University Press, 2000), 25.

absolutely dependent upon the practical ability to establish and maintain the *identity* of its members. Regardless of the type of group or the specific means of establishing membership, each membership group is defined by its ability to identify those which properly belong to it. If a membership group cannot identify its members, there is simply no group. It is the act of monitoring membership through the establishment of credible identities that, on the one hand, compromises the privacy of the individuals involved, and on the other hand, produces the conditions for the possibility of implementing security. One need only consider the exponential growth in cases of so-called "identity theft" to recognize not only the importance of maintaining verifiable identities within a membership group, but also that the threat posed to institutions that provide security through membership is the increasingly likelihood that such institutions may not, in fact, know who their proper members are.

III

The model I am presenting here need not be as complicated as it may seem. A few examples will help clarify the point. Consider the most common of security devices, the padlock. The fact that I, as the owner of the lock, also possess the key which opens it, attributes to me a very specific identity with respect to the security provided by the lock. The lock, in effect, "recognizes" me as being the legitimate owner of the lock because I have a key which verifies my identity. The key, in other words, acts as what is known as an "identity token." However, if someone steals my key and uses it to open the lock without my permission, they have thwarted the security provided by the lock precisely by, at least as far as the lock is concerned, feigning my identity. Or put differently, they have feigned membership in the rather small security organization which includes myself and, say, the other members of my family who also have copies of the key. Admittedly, if someone breaks out a hammer and manages to bust the lock to pieces, the security provided by the lock has been compromised by means other than feigning identity, but my concern is not to prove that brute force is not a security risk, but rather to show that identity is always a significant component of security. When one opens a lock with a pick, he or she is, above all, feigning identity.

To take another somewhat clichéd example, consider the case of a spy. A spy spends years learning how to access classified information not by directly assaulting the safe in which the material is kept, but by accumulating the criteria, i.e., the "identity tokens," which allow him or her to fake membership and thereby gain access. Unlike the lock and key example, the case of the spy involves a far more complex set of factors. Not only does the spy need, for instance, a password or a key to access the secured information, he or she also needs to develop a wide range of often non-technical characteristics in order to gain access, for instance, to certain meetings or certain trusted conversations. The spy must breech security not only explicitly by acquiring a password, but implicitly by slowly developing trusted friendships and professional relationships with those who either possess the information themselves or represent a means to acquiring that information. The set of techniques used to enter the trust of another person are important aspects of any security system because at its most basic level the establishment of *trust*, when done disingenuously, is a common form of feigning membership.

To take an example from the world of computer hacking, it is too often assumed that malicious entry into a computer system is purely the result of programming skills. In fact, much of the information necessary to breech a computer system is accumulated by hackers directly from those who are fully authorized to access it. By feigning the identity of, say, a fellow employee schooled in the specific acronyms and terminology of a particular type of business, it is quite possible to casually convince a legitimate user to surrender his or her password. More often than not all that is needed is a simple phone call. Here, as with the spy example, the breech of security occurred *long before* the computer account was explicitly accessed. For instance, it was the feigning of membership—in a governmental institution and a private business—that led to direct access of secured material. This method for manufacturing the trust that legitimately exists between those associated by membership to a membership group has, at least in the world of hacking, a very specific and recognized name. It is called "social engineering."

Before moving on to my final example, it is important to say a word about a term that played a crucial part in the previous two examples, namely, *access*. Put simply, *security is always a matter of access*. Despite the seeming incongruity between securing and accessing, the two terms are inseparable, and not simply because they are reciprocally defined. An example I recently used with my students in a course on the subject makes this quite apparent. While sitting around our conference table I made the claim that security is first and foremost a question of access. After receiving quizzical looks from around the table I asked the

students to play along with a simple scenario. Let us say I have a safe in front of me in which to secure some items of value. I asked my students what items we should secure and within a few moments we decided that it should be our money. So I asked them to give me their money (hypothetically, of course) so that I could place it in the safe. I then told them I would lock the safe and, to be sure it was totally secure, I would throw it into the nearby Chesapeake Bay. The point of the exercise reveals itself rather quickly. While the money would certainly be secure, for hundreds of years perhaps, it does us no good if we, the rightful owners, cannot access it. It is, in other words, easy to secure something if you never need to see it again. The difficulties arise precisely over the question of how an object can be both secure and accessible at the same time. And this is where identity within a membership group becomes essential. Only by being able to accurately identify who should, and who should not, be permitted to gain access to secured items can a secure system hope to be viable.

Turning now to my final and far less obvious example, an example which sits squarely in the gray area between that which is and that which is not a compromise of security, consider the all too familiar occurrence of a telemarketer's evening phone call. The goal of the telemarketer is, of course, not to steal anything from you (as was the case with the spy and the hacker), but to sell you a product. Thus, from the outset the stakes are different. But as we saw in the two preceding examples, the breech in security happened well before the spy accesses the documents or the hacker enters the computer. The breech, as I suggested, happened at the level of building a false sense of trust within a membership group of which one was not a legitimate member. Perhaps not surprisingly, the techniques used by the telemarketer to gain access to your wallet by persuading you to willingly part with your money are very similar to those used by the spy or the hacker, with the critical difference that the telemarketer must acquire *legitimate consent* from the customer. That is to say, the telemarketer must persuade the potential customer to give away his or her money in exchange for a product or service without falsely representing that product or service. In the case of the hacker, a password was freely given away and consent was freely given to access the information secured by that password, but the intentions of the hacker were not legitimately represented and therefore the consent can also be considered illegitimate. Telemarketing, and for that matter all permission-based marketing, functions by establishing a level of trust with customers based on more or less legitimate representations of both products and intentions. To the extent that marketing campaigns can exaggerate or obscure information regarding either their products or their intentions (particularly with respect to personal information acquired from consumers), they can legally intrude deeply into personal privacy.

It is common for the telemarketer to use the first name of the person he or she is calling, for instance, "Hi Steve, this is Tom from Acme Insurance. How are you doing tonight, etc. etc." The salesperson uses this informal mode of address as a means of quickly achieving a level of familiarity with the person who answers the phone, thereby gaining trust, and with it an increased likelihood that the person will believe the sales pitch and purchase the product. Viewed from the vantage of what has been discussed above, however, this scenario is simply another example of an attempt to feign membership, in this case membership into that membership circle (usually characterized by deep trust and, therefore, substantial security) called friendship. That marketing agencies pursue this type of feigned familiarity is beyond doubt. One need only turn to Seth Godin's recently published book on direct-marketing, unambiguously entitled, *Permission Marketing: Turning Strangers into Friends and Friends into Customers*,[11] to get a strong idea of how marketing functions as a type of "social engineering." Godin, one of the world's foremost online promoters, argues that gaining *permission to market to a customer* is the key to sales. Persuaded with some kind of bait—a free sample, a supermarket discount card, a contest, an 800 number, or even just an opinion survey—once a customer *volunteers* his or her time, sales are more likely. Be it a spy, a hacker, or a direct marketer, the process of "turning strangers into friends" is central to feigning membership so as to exploit the power of trust. While the legitimate consent given by the consumer to have the salesperson debit his credit card account keeps this practice on the legal side of the security line, the techniques utilized in the process of making the sale are quite similar to those used to breech security in less legal endeavors.

The media by and large functions in a similar manner, with the added distinction that what the media sells is not a product or a service that *follows from* the establishment of a congenial, or to use Godin's terminology, a friendly relationship or trust, but is *that very relationship itself*. The media lives and dies by its audi-

[11]Consider a book by Seth Godin, a direct-marketing expert, entitled, *Permission Marketing: Turning Strangers into Friends and Friends into Customers* (New York: Simon & Schuster, 1999).

ence, e.g., its readership, viewership, etc., and consequently the very existence of the media is dependent upon the decision on the part of private individuals to "tune-in" to the stream of information or entertainment that is being offered. Unlike the sale of stoves and tennis racquets, however, the media has a uniquely important role to play with respect to the functioning of democracy. It is widely conceded that in order for a democracy to function properly, its citizenry must be kept reasonably informed of the important issues of the day. Democratic participation—making an informed judgment not only when voting, but also in local civil actions—necessitates the existence of a fair and relatively unbiased media whose duty it is to provide people with relevant information. To the degree that the media is also in the business of selling the relationship it has with its audience, however, the risk that the media is able to shape the views of its audience, due in part to their loyalty as members of this loosely conceived membership organization of viewers, remains significantly high. And this is especially worrisome when one realizes that the product the media is selling to its audience, the programming, is the very means by which the media attempts to establish a loyal viewership, i.e., a loyal membership of consumers. It is this "relationship of trust" that serves as the foundation of the media's dependable audience, but it is also this trust that presents the media with the dangerous opportunity to manipulate the opinions and desire of its audience by distributing leading or biased programming.

To sum up, then, it is my contention that many, if not most, security threats (not to mention successful marketing campaigns) can productively be understood as a form of forged membership. If one can convincingly become a member of a group without buying into the initial "contract" that establishes that group's legitimate members, then one poses a direct threat to the principles of stability that the contract seeks to maintain. A membership organization functions, first and foremost, by keeping track of its members. It is this monitoring, something which is a critical part of all security, that inevitably makes inroads into one's privacy. At the most basic levels, this trade-off is quite acceptable. In the case of political membership, we give up the complete autonomy bequeathed to us in the "state of nature" by becoming members of the state which in turn provides us with reasonable assurances of safety. But the trade-off becomes more difficult the more aggressive the state becomes in monitoring our behaviors, so much so that the information which once served as the very condition for security becomes a security risk itself. And this is where the utilitarian consideration of harm arises. At what point does our desire for security become overshadowed by our desire for privacy? In the case of the Fourth Amendment, for instance, the state is barred from "unreasonable searches and seizures." While it would, given a trustworthy government, undoubtedly be a more secure society if the state could enter our private households at will to check for illegal property or potentially harmful activity, most of us recoil at such an idea. The reason for this is that our desire to maintain a high level of privacy within the space of our homes greatly outweighs the benefits that would result from unhindered governmental searches. In other words, the harm caused by the invasion of privacy convincingly outweighs any benefits that might be a consequence of such an intrusion. Thus, the amount of privacy and security we wish to have presents itself in the form of a classic moral dilemma in which these significantly contrary goods must be brought into balance. However, in the case of non-governmental organizations, and businesses and the media in particular, the trade-off is less clearly one between privacy and security. Indeed, if businesses and the media are concerned about security at all it is with *their own* financial security, which makes a business's or the media's intrusion into our private lives, as opposed to that of the state, far more risky than we often presume.

IV

As we have seen, the modern form of the Western nation state is based upon a security relationship which, at least in theory, seeks to preserve individual autonomy and the privacy that characterizes it. Individual privacy, in the form of both private property and one's own body, is that which is deemed worthy of being secured, while the public sphere is represented by an authority that enables security precisely through its right to legitimately intervene into the private sphere (both physically and informationally) to prevent, manage, or punish instances of intentional harm. The price paid by the individual for residing in this state of security is the regulated intrusion into his or her private affairs, as well as the requirement that one become and remain a member of a collective (i.e., a public) organization. Likewise the form of punishment very often incurred by those who injure others and thereby infringe upon their personal privacy is precisely a loss of their own personal privacy insofar as imprisonment entails, in conjunction with confinement, a continuous state of surveillance of personal activities.

While the United States Constitution does not explicitly recognize a right to privacy, two Amendments are often cited in support of such a right.[12] The First Amendment, which guarantees the freedom of religion, speech and assembly, appears to implicitly entail a right to privacy insofar as the freedom to engage in self-expression seems to presuppose that such expression is permissible out of view of the public gaze. The Fourth Amendment, on the other hand, has been shown to recognize privacy rights based on property in as much as it guarantees the "right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures." The trouble with this claim is, of course, that the force of the argument turns on what exactly one considers property. In their 1890, groundbreaking article "The Right to Privacy," Samuel D. Warren and Louis D. Brandeis set forth the first fully conceived statement by the court concerning privacy rights. In the article, they argue that fundamental rights to life, liberty, and property must include not only the physical manifestations of these rights, but also their less tangible forms. As Warren and Brandeis put it, "the right to life has come to mean the right to enjoy life—the right to be let alone; the right to liberty secures the exercise of extensive civil privileges; and the term 'property' has grown to comprise every form of possession—intangible as well as tangible."[13] The upshot of their argument is that it pushes the law beyond a collection of torts, drawn largely from common law, which address specific issues of privacy, towards a recognition that the violation of privacy is a tort itself. In other words, to take an example from an article by A. M. Capron, instead of crafting a special provision to legally institute the prohibition against, for instance, eavesdropping (literally listening to a conversation within a private house by standing as close to the house as rain falling from the eaves), which had long been recognized in common law, the Warren-Brandeis documents distill all matters of privacy violation into four basic areas.[14] In an article written many years after the Warren-Brandeis piece had become a benchmark for the courts, William L. Posser summarized the four basic categories of privacy as follows:

1. Intrusion upon the plaintiff's seclusion or solitude, or into his or her private affairs
2. Public disclosure of embarrassing private facts about the plaintiff
3. Publicity which places the plaintiff in a false light in the public eye
4. Appropriation, for the defendant's advantage, of the plaintiff's name or likeness[15]

The fourth category is of particular importance in as much as it speaks directly to the issue of assuming an identity for the sake of gaining access to the membership group the plaintiff is associated with. However, it is the first category that implies the most broad reaching violations of privacy rights.

While one would not have to work hard to convince most people that the government has no right to track the goods we buy or to monitor what television programs we watch without just cause, it is not so clear that non-governmental organizations, particularly businesses and private media consortiums, do not have such rights. As a matter of course, supermarkets, cable television operators, credit card companies, Internet service providers, and the like, all engage in activities which pry directly into the most private aspects of our lives—from the programs we watch to the food we eat. Each of these organizations, then, regularly intrudes upon what Posser referred to as our "private affairs." The "assumption of privacy" that many of us instinctively adopt when we are within the confines of our homes may not be as valid an assumption as it once was. When one is able to watch events in real time piped through cables into our living rooms, or when we are able to sit at home and access information stored thousands of miles away via an Internet connection, is it still reasonable to assume that these are private activities? By and large, Americans feel that the entertainment we engage in within our homes and the information we access for personal reasons ought to remain within the private sphere. We feel violated, in other words, when we realize that strangers know what programs we watched last night; we are troubled to know that

[12] In addition to these two Amendments, the Ninth Amendment, which claims that "the enumeration in the Constitution of certain rights shall not deny or disparage others retained by the people," is often cited in defense of privacy claims.

[13] Samuel D. Warren and Louis D. Brandeis, "The Right to Privacy," *Harvard Law Review* 4, no. 5 (1890), 193–220. Reprinted in *Philosophical Dimensions of Privacy: An Anthology*, ed. Ferdinand David Schoeman (Cambridge: Cambridge University Press, 1984), 75.

[14] A. M. Capron, "Genetics and Insurance: Accessing and Using Private Information" in *The Right to Privacy*, ed. Ellen Frankel Paul, Fred D. Miller, Jr. and Jeffrey Paul (Cambridge: Cambridge University Press, 2000), 239.

[15] William L. Posser, "Privacy," *California Law Review* 48, no. 3 (1960), 389. Quoted in Capron, "Genetics and Insurance," 240.

Internet sites place "cookies" on our computers so as to better monitor our online behaviors. Ask people if they would feel comfortable with anyone knowing exactly what they purchased in the last six months and many would cringe. In the same way that many people feel that the government's right to search our private property ought to be limited by law, is it not reasonable to expect private corporations and media companies to adhere to similar, though perhaps less stringent, restrictions? Especially because unlike the government, businesses have no explicit mandate (no "social contract") to keep the best interests of their customers in mind.

Businesses and media conglomerates are growing increasingly inclined to gather as much information about their customers as possible and to use that information in complex ways, not only to tailor their inventory to the desires and habits of their customers, but, through direct marketing, to actively produce desires within certain predisposed demographics. As David Potter sagaciously argued in his 1954 book, *People of Plenty*, marketing is "the only institution which we have for instilling new needs, for training people to act as consumers, for altering men's values, and thus for hastening their adjustment to potential abundance."[16] Potter's statement could hardly be more relevant than it is today, not only because our level of abundance has never been higher, but because the means at the disposal of marketing firms to track, as well as shape, the behaviors of consumers has never been more powerful. While businesses and media companies have always sought to woo their customers and audiences by gathering information about their lives and their interests, the past several decades have seen this practice raised to a new level of efficiency, efficacy, and invasiveness. With the introduction of electronic means of data collection and information management it has now become feasible to track each transaction within a business, associate those transactions with specific customers, and then compare the information with databases collected by other businesses so as to build a relatively complete picture of a relevant customer base. Likewise, the media, by tracking each cable show we watch, and by measuring how long and how often we visit Web sites, will soon be able to tailor entertainment, as well as news and informational programming, to specific individuals and households. The traditional model of media "broadcasting" is quickly being replaced by a new model, "narrowcasting," where streams of information are directed to both specific individuals and well-isolated demographics. *Time* magazine, to take but one example, already employs such a technique, called "cluster analysis," to group individuals according to behavioral and socio-economic similarities. It then uses the information gained in this process to target its publications, or more specifically the ads within its publications, to specific "market segments." Consequently, the issue of *Time* you receive at home does not contain the same advertisements as those received by other individuals identified as being within a different market segment.[17]

While media companies claim that target marketing is being done in the interest of providing the consumer a more "customized" array of services, and while this may, to some extent, be in fact true, it is not at all clear that the consumer, if he or she knew the amount of personal information which had been gathered about them, would be willing to trade this accumulation of private information for the convenience promised. Here, then, the relationship between privacy and security shifts to that between privacy and *convenience*, and I believe it is this trade-off that harbors for us the most important questions regarding the value of privacy for the new century. The question, in other words, is no longer how much privacy are we willing to sacrifice for the sake of security, but how much private information we are willing to sacrifice for convenience. The shift is a crucial one. In the case of the privacy/security trade-off, the state's intrusion into the private lives of individual citizens was done, at least in theory, for the sake of those citizens and their safety. The state, in other words, was established to protect people from unjustified harm in their private lives. In the case of non-governmental businesses and media companies, however, the safety of individuals is not a primary concern. When a business gathers private information on its customers it is not doing so with the intention of protecting these customers from harm, so much as it is doing so to keep ahead of its competition and to generate sales revenues. It is ultimately for its own sake, for the sake of its own financial survival, which is to say, for the sake of its own security, that a business accumulates personal customer information, even though the consumer is quite often the recipient of certain benefits. Without a fundamental

[16]David M. Potter, *People of Plenty: Economic Abundance and the American Character* (Chicago: University of Chicago Press, 1954), 175.

[17]Oscar H. Gandy, Jr., *Operation the Panoptic Sort: A Political Economy of Personal Information* (Boulder: Westview Press, 1993), 88.

mandate to keep the consumer's interests in mind, that is to say, without being bound, like the state, to a "contract" which explicitly empowers the individual and his or her rights with respect to privacy, the risks of seeing one's personal information used to one's own disadvantage are significantly greater.

Consequently, as the debates about privacy move into the next century, it is primarily the trade-off between privacy and convenience that must be scrutinized. The terms of the debate which occupied thinkers such as Hobbes and Locke, namely, the balances of power between the individual and the state, have certainly not lost their relevance, but it is becoming increasingly clear that business and media interests must be directly factored into the discussion. When corporations can operate seamlessly across vast transnational territories in pursuit of their own institutional interests, it is essential to reevaluate the terms of the privacy debate with respect to the often incompatible interests of individuals, states, and corporations as well as to renegotiate the issues of membership and identity embedded within them.

Discussion and Reflection Questions

1. What is "privacy"? Is there a fundamental right to privacy? How might one argue for such a right? How might one argue that there are limits to an individual's right to privacy (e.g., when it conflicts with some greater common good)?
2. How might a conflict arise between (a) the desire to live in a society where individual privacy is guaranteed, and (b) the desire to live in a society safe from criminal activity? How might these two desires be balanced against one another to form the best compromise?
3. DeCaroli describes the "assumption of privacy" that many of us instinctively adopt when we are within the confines of our homes, and notes that it may not be as valid as it once was. Why not? How does modern technology call into question the idea that what we do in the "privacy" of our own homes is not really as private as we might like to think? Do you find this a cause for concern? Why or why not?
4. DeCaroli notes that in some ways the issue has shifted from how much privacy we are willing to sacrifice for security to "how much private information are we willing to sacrifice for convenience?" In the context of the examples he discusses, how would you answer this question?

Suggestions for Further Reading

For materials that work through a range of ethical considerations in mass media, see *Mass Media and the Moral Imagination,* edited by Philip J. Rossi and Paul A. Soukup (Kansas City, Mo.: Sheed and Ward, 1994); S. Klaidman and Tom L. Beauchamp, *The Virtuous Journalist* (New York: Oxford University Press, 1987); *Democracy and the Mass Media,* edited by J. Lichtenberg (Cambridge: Cambridge University Press, 1990); John M. Phelan, *Disenchantment: Meaning and Morality in the Media* (New York: Hastings House, 1980); Ralph L. Lowenstein and John C. Merrill, *Macromedia: Mission, Message, and Morality* (New York: Longman, 1990); *Communication Ethics and Universal Values*, edited by Clifford G. Christians and Michael Traber (Thousand Oaks, Calif.: Sage, 1997); Matthew Kieran, *Media Ethics: A Philosophical Approach* (Westport, Conn.: Praeger Publishers, 1997). To assist in the exploration of ethical issues in journalism, see *The Journalist's Moral Compass: Basic Principles*, edited by Stephen R. Knowlton and Patrick R. Parsons (Westport, Conn.: Praeger Publishers, 1994); *Committed Journalism: An Ethic for the Profes*sion (2nd edition), edited by Edmund B. Lambeth (Bloomington: Indiana University Press, 1992); *Moral Reasoning for Journalists: Cases and Commentaries*, by Stephen R. Knowlton (Westport, Conn.: Praeger Publishers, 1997); John C. Merrill, *Journalism Ethics: Philosophical Foundations for News Medi*a (New York: