International Journal of Philosophy and Theology
March 2014, Vol. 2, No. 1, pp. 93-118
ISSN: 2333-5750 (Print), 2333-5769 (Online)

American Research Institute for Policy Development
42 Monticello Street, New York, NY 12701, USA.
Phone: 1.347.757.4901 Website: www.aripd.org/ijpt

Before Snowden: Privacy in an Earlier Digital Age

Jennifer K. Greene[1]

Introduction

With the recent revelations of surveillance by the National Security Agency (NSA) privacy is once again in the spotlight. The current collection of personal data, including emails, internet searches, credit card transactions, phone calls, and more, is however, just the latest in a series of alleged privacy violations. Full body scans at airports, biometric facial recognition, "no refusal" traffic stops, and many other forms of search and surveillance have been the subject of outrage on the part of citizens since the creation of the internet and the attacks of 9/11.Americans are being watched and they don't like it. Yet, as the methods by which privacy can be invaded proliferate, so have measures to counteract perceived violations.While Edward Snowden's disclosures and their aftermath are riveting and obviously in need of extensive evaluation—legally and ethically--this paper will focus on privacy concerns for which we know not only the incursions but the responses to them as well. More specifically, the focus of this paper will be the efficacy of past responses to privacy incursions and what they tell us about the meaning, value, and even existence of privacy.

[1]PhD, Associate Professor of Philosophy, St. Edward's University, Austin, TX 78704, USA.
Tel: 512-428-1341

Like the NSA affair, the cases to be analyzed concern the citizen, the government, and personal information. Among the most ambitious (and costly) measures to protect citizens' privacy are two recent measures passed by Congress—the Final Privacy Rule of the Health Insurance Portability and Accountability Act (HIPAA) and an amendment to the Final Rule on Privacy of Consumer Financial Information—designed to protect privacy of medical and financial information respectively.Each Rule is a response to the exponential growth of personal information resulting from digitalization of records and the consequent number of people who can see them; there's more to go around and many more players in the game. Both Rules are designed to limit access and regulate distribution.

At first glance, it looks like such measures are a reasoned response to a serious attack on a fundamental aspect of our well being as citizens, and in some cases that may well be the case. I want to suggest, however, that in many instances we are suffering from a serious confusion over the meaning—and hence, value—of privacy, and that such confusion may well be leading us to take pointless precautions on the one hand, and more importantly, fail to safeguard real privacy on the other. We seem moreover to be ambivalent about its value and thus unclear as to how best to secure it. A brief examination of the structure and efficacy of the two major pieces of privacy legislation regarding medical and financial records will illustrate my first claim—that we are barking up the wrong tree with regard to privacy protection. I use these Rules as examples both because they are the most costly and far-ranging attempts at shoring up privacy to date, and because they represent what has become the paradigmatic approach to privacy in the digital age namely, abundant disclosure, but with permission. As evidence for the plausibility of my second claim—that we may be failing in important ways to protect privacy—I focus primarily on governmental responses to events following the September 11thterrorist attack.

There seems to be, then, both more and less concern over (and protection of) privacy in contemporary society. After reviewing these parallel developments, I turn to the heart of my argument: the meaning and value of privacy itself. For it is, once again, confusion over these basic issues that makes it possible for us to adopt seemingly contradictory positions regarding privacy. We know we like it and should cherish it, but what precisely is it? Moreover, what are we willing to give up in order to secure it? While the literature on privacy is sizeable, I suggest that important developments in the ways and conditions under which we make bids for privacy justify revisiting the issue.

More specifically, advances in technology, communication, access, and mobilization have radically changed the way in which we view our personal lives, information about ourselves, and privacy in general. And as Fred H. Cate states, "the demand for, and contours of, privacy differ significantly depending upon the level of development in a society."[2] Our responses to invasions of privacy, then, ought to change with the times; but that change can only be accomplished effectively if we know the nature and value of what it is that we are trying to protect.

Part One: Privacy in the Modern World

False Protections: Privacy vs. Data Security

In this section, I briefly review two recent attempts to shore up our privacy: the Final Privacy Rule of HIPAA and the Financial Information Act, an amendment to the Gramm-Leach-Bliley Act. Both pieces of legislation purport to provide greater privacy protection for individuals through the regulation and distribution of personal information with regard to medical and fincancial data respecitively. I will argue that both miss the mark, at least in terms of protecting *privacy*; yet there nevertheless appears to be considerable confidence in the efficacy of the Rules. My first question is what is it that these Rules are really accomplishing? And secondly, is that accomplishment really related to privacy? A sketch of each of the Rules is necessary to answer these and other questions.

---

[2] Fred H. Cate, *Privacy in the Information Age* (D.C.: Brookings Institution Press, 1997), 22. This sentiment was echoed by Samuel D. Warren and Louis D. Brandeis in their famous essay which essentially introduced the legal right to privacy: "The narrower doctrine [of protection from the invasion of others] may have satisfied the demands of a society at a time when the abuse to be guarded against could rarely have arisen without violating a contract or a special confidence; but now that, modern devices afford abundant opportunities for the perpetration of such wrongs without any participation by the injured party, the protection granted by the law must be placed on a broader foundation." "The Right to Privacy: The Implicit made Explicit," in *Philosophical Dimensions of Privacy*, Ferdinand D. Schoeman, ed. (Cambridge University Press, 1984), 84.

Medical Privacy

Briefly, the HIPAA Final Privacy Rule identifies three different sorts of participants involved in the provision of health care: covered entities, business associates, and the individual (the patient who is the subject of the protected information). Covered entities, by far the broadest and most important category, include any person or business which is involved in the provision and payment of health care or so-called "health care operations." The latter category alone (health care operations) includes:

> quality assessment and improvement activities, … Reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance, health plan performance, conducting training programs …Underwriting, premium rating and other activities relating to the creation, renewal or replacement of a contract of health insurance or health benefits …Conducting or arranging for medical review, legal services, and auditing functions, … Business planning and development … Business management and general administrative activities …[3]

Business associates are defined as agents of the covered entity, providing such services as legal, actuarial, management, data aggregation, and financial services among others.[4] And the individual, as just stated, is the subject of the information, the patient.

The basic thrust of the Rule is that disclosure of personal health information between covered entities for the purpose of providing, paying for, and administering health care is permitted only if consent from the subject of the records has been obtained. The business associates operate under the general umbrella of health care operations, but being an agent of the covered entity rather than the patient, are answerable only to the former. The regulations are complex and allow for a number of exceptions (such as emergency care when consent is often unobtainable), but this is the basic idea—the information is only shared with the subject's consent. Initially this sounds as though the protection provided is substantial indeed. However, there are several further details to consider before rendering final judgment.

---

[3] Final Privacy Rule – Regulation Text, Federal Register: 12/28.00 (Volume 65, Number 250), §164.501.

[4] Id., at §160.101.

I investigate that evaluation after a brief sketch of the legislative protection offered for financial privacy.

Financial Privacy

The second piece of privacy legislation, the Final Rule on Privacy of Consumer Financial Information, was issued by the Federal Trade Commission (FTC) in 2000 in accordance with the Gramm-Leach-Bliley Act.[5] As described by the FTC, "Under these provisions, financial institutions have restrictions on when they may disclose a consumer's personal financial information to nonaffiliated third parties."[6] Like the HIPAA Rule, this Rule seeks to *regulate* disclosure rather than prevent it. After defining financial institutions, customers, and consumers (along with numerous other terms), the Rule lays out the conditions under which a financial institution may share, and even sell or rent, "Nonpublic Personal Information" with non-affiliated third parties. Essentially, any institution wishing to share such information must have provided its consumers and customers with the opportunity to "opt out," that is, to refuse to allow such disclosure.[7] Financial institutions are also required keep their customers apprised of their privacy policy, including notifying them of any changes.[8]

---

[5] Public Law 106-102, 15 U.S.C. § 6801, et. seq.

[6] "Outline of The Gramm-Leach-Bliley Act: Privacy of Consumer Financial Information," <http://www.ftc.gov/privacy/glbact/glboutline.htm> (2/10/02).

[7] Financial institutions fulfill this requirement by sending out mandatory privacy statements outlining the entities with whom information will be shared. It is common knowledge that these notices are virtually unreadable (and hence, unread), littered as they are with jargon and long enough to cover all potential liability. However, there have been two welcome additions in this regard: the Financial Service Requirement Relief Act of 2006 which requires agencies to issue a "*succinct* and comprehensive form"; and the Final Model Privacy Notice Form of 2009, which standardizes and simplifies the format of the disclosure.

[8] There are slightly different requirements imposed upon the financial institutions depending on whether the Nonpublic Personal Information concerns a consumer ("an individual who obtains … a financial product or service … that is to be used primarily for personal, family, or household purposes") or a customer ("a consumer who has a 'customer relationship' [on-going] with a financial institution"), but such distinctions are unimportant for our purposes (id., at 3, 4).

Notices informing consumers of privacy policies and practices, in addition to offering the opt-out alternative, must list for the individual the types of nonpublic information collected, which portion of that collected data is disclosed, the *type* of entity (rather than the specific identification) to whom it is disclosed, its "policies and practices with respect to protecting the confidentiality and security of nonpublic personal information,"[9] and if it chooses, the reserved right to disclose to other nonaffiliated third parties not currently listed.

As with the HIPAA Privacy Rule, there are many more details to be filled in, but for our purposes this sketch suffices. The basic idea is that financial institutions may not share individuals' private information with nonaffiliated third parties without a) letting those individuals know that they are doing so (or may do so), and b) giving the subject of the information an opportunity to prevent such disclosure by opting out. Again, at first glance such a scheme seems salutary. Again, its protections regarding privacy may be less impressive on closer inspection.

Analysis of Rules

Both Rules concerning privacy represent massive efforts by the Congress and the industries involved to offer consumers greater security while at the same time preserving the industries' ability to carry on business. In other words, in framing such policies the authors have of necessity performed a balancing act; security and efficiency, privacy and business, protection and payment, have all been weighed against one another and the resulting Acts are offered as the compromise solutions. Unsurprisingly, advocates of the Rules hail their ability to protect the individual while critics claim they accomplish little. While I do not intend to offer any more detailed analyses on industry-specific claims, there are a number of parallel weaknesses in the Rules which are worth mentioning in response to the more conceptual question of how much we are getting right in contemporary society with regard to privacy protection.

Prior to that assessment , however, a brief detour is necessary. For in order to assess the efficacy of such Rules, we need a working characterization of that which they allegedly protect, namely privacy. As mentioned in the introduction, the literature on privacy is vast.

---

[9] Id., at 9.

This is so not only because privacy is considered fundamentally important to free and legitimate social, legal, and political arrangements and institutions, but because it is a multifaceted concept which eludes easy definition. For privacy applies to a curious mix of disparate acts, events, things, states of mind, and information. We speak of privacy with regard to our body parts, personal papers, important life decisions, financial status, homes, genetic inheritance, past actions, and our physical selves even when out in public, to name just a few examples. Moreover, privacy is said to be intimately related (again in disparate ways) to a host of other values, including freedom, intimacy, autonomy, integrity, respect, dignity, trust, and identity.

As a result of these widely varying applications, many theorists claim there are distinct *kinds* of privacy. For instance, Judith Wagner Decew argues that there are three types of privacy which she labels informational, accessibility, and expressive privacy.[10] Ferdinand Schoeman, on the other hand, claims there are just two sorts of what he calls "privacy norms": those which protect our expressive roles and those which attach to types of behavior.[11]And William L. Prosser argues that the magic number is four, at least in legal terms.[12] Fortunately, for our purposes it is unnecessary to enter the philosophical fray regarding the precise taxonomy of the concept or the specific way in which it is related to other important values. Rather, I shall approach the question of privacy's meaning in an empirical fashion, beginning with undisputed incidences of privacy protection or violation, and only then going on to examine what is at stake in such cases.[13] I mention these different interpretations, however, to point to the important fact that the concept we are dealing with is complex indeed—answers regarding its protection in a highly developed society such as ours will not come easily.

Once again, in order to assess the Privacy Rules, we need at least a working characterization of the sort of good allegedly at stake.

---

[10]*In Pursuit of Privacy: Law, Ethics, and the Rise of Technology* (Cornell University Press, 1997). She writes that there are "three related clusters of claims concerning information about oneself, physical access to oneself, and decision making and activity that provide one with the independence needed to carve out one's self-identity through self-expression and interpersonal relationships." 78.

[11]*Privacy and Social Freedom* (Cambridge University Press, 1992),14-19.

[12]They are: "1. Intrusion upon the plaintiff's seclusion or solitude, … 2. Public disclosure of embarrassing private facts … 3. Publicity which places the plaintiff in a false light … 4. Appropriation … of the plaintiff's name or likeness." "Privacy [a legal analysis]" in Schoeman, 1984, 107.

[13]In the second part of this paper, I shall add a further, but still empirical, element to the definition or characterization of privacy, namely a teleological one.

And this turns out to be a fairly straightforward question. The focus of the financial and medical Privacy Rules is information. More specifically, we are concerned about *who* may have access to information which is specifically about us and which could lead to others treating us differently—better or worse—as a result of obtaining the information. This is generally agreed to be what is known as "informational privacy" and is importantly about *control* over what others may know of us, not just about blocking knowledge as such. As Charles Fried explains, "To refer, for instance, to the privacy of a lonely man on a desert island is to engage in irony. The person who enjoys privacy is able to grant or deny access to others."[14] Thus, what we are interested in with regard to the Privacy Rules is *how much* control over sensitive information they afford the subject.Moreover, given that this is a quantitativequestion, it's worth asking whether we are even talking about privacy anymore.

To begin with the medical case, both the health care provider and the health plans are allowed to *condition* treatment and enrollment respectively on the consent of the patient.[15] But since they are not allowed to disclose any information absent consent (except under a few relatively infrequent circumstances), it is unlikely that any provider would agree to treat a patient who refused consent unless he paid out of pocket. And a health plan which is not allowed to share medical records will not be long for this world. Thus, it will be difficult at best to find treatment and coverage unless one is willing to sign the consent form. Whether this amounts to coercion or not will depend on one's understanding of the meaning of that term (in particular whether it is interpreted normatively or descriptively). But whatever one's judgment on that issue, allowing for treatment only with consent does make that consent substantially less voluntary and hence, less impressive in terms of the control retained by the individual.

The Privacy Rule in the financial realm suffers from a different weakness, but one which has similar results to the conditioning of treatment in the medical Rule. The aspect of the financial scheme which can minimize control and maximize access is the fact that limits on disclosure are made through an "opt-out" system rather than an "opt-in" one.

---

[14] *An Anatomy of Values: Problems of Personal and Social Choice* (Cambridge: Harvard University Press, 1970), 140.

[15] §164.506 (b).

What this means is that the subject of the information has to take positive action in order to prevent sharing of his information by sending in a form which effectively prevents the financial institution from sharing with non-affiliated third parties. In other words, the system defaults to sharing (which, once again, often means selling or renting) information and only prevents it when the customer takes positive action. The opt-out rates are notoriously low, indicating that such action is not forthcoming from the vast majority of the population. Of course, this might mean that the most consumers simply do not mind having their information sold to third parties; but if this is the case, it is difficult to say why we are engaged in such cumbersome and costly legislation in the first place.

Finally, when considering the degree of control over information afforded to the individual, it is important to keep in mind just how many parties are legitimately allowed access to protected health and financial information under the Rules. As the list of health care operations makes clear, that number is not negligible. Moreover, the layer of administration required to complete the payment process is obviously extensive as well. The situation with financial records is, if anything, worse. For the Rule there provides no limits at all to the sharing of information between affiliates; rather it applies only to non-affiliated third parties.The primary purpose of the Financial Services Modernization Act (the GLB Act) was to create what are known as "financial supermarkets"—entities which may combine banking, securities and insurance services. One obvious effect of such mergers is to increase the number of parties who will count as affiliates, thus enlarging the sphere in which financial information may be legitimately shared without the subject's consent *or knowledge*. Given that treatment and coverage can be conditioned on the consent to share medical information amongst covered entities on the one hand, and that the financial privacy regulations say nothing about sharing amongst affiliates, on the other, the degree of control individuals retain over their personal information is in fact quite minimal.

Thus, our financial and medical information travels far. The question is whether it is really with our blessings. We have seen that consent to share medical information is, at the very least, questionable if treatment is predicated on it. Similarly, the failure to opt out in the financial case is hardly a model of voluntary, informed consent.

Given the complexity of the systems, it's unlikely that anyone could point to the "business associates" or "financial supermarkets" reviewing their personal information. But if this is so—if consent to share doesn't include knowledge of those who are privy—there is little left of the normative value of privacy. Recall that the term is often defined through other concepts such as autonomy, identity, dignity, and freedom. The Rules which govern the dissemination of personal information in a networkwhich is both vast and difficult to understand standardize and regulate the procedures, but they do not promise any of the things we value privacy for. They certainly don't protect us in the creation of our own persona; nor do they leave us autonomous because we have "agreed" to share.

Part Two: Another Look at Privacy

The Meaning of Privacy

As already mentioned, the literature on the concept of privacy is substantial indeed, yet differences of opinion remain.[16] As in my review of privacy protections and incursions, I adopt an empirical approach, asking initially how does privacy work rather than what it is in the abstract. More specifically, I examine the components of a privacy claim: the time and place of the privacy claim (or invasion), the individuals against whom privacy is demanded, and the purpose of the bid to privacy in the first place. My argument is that given the central role of context in assessments of valid privacy claims, radical changes in the former will call for a new understanding of the latter. But this is just what we have failed to take into account in our current responses to privacy violations. Our ineffective privacy measures may well be the result of working with an outmoded understanding of privacy.

[16] Interestingly, however, very little work on the concept has been done since the seventies and eighties, with the exception of Adam D. Moore, who himself relies on much earlier sources. See "Defining Privacy," *Journal of Social Philosophy* 39 no. 3 (2008): 411-428 and *Privacy Rights: Moral and Legal Foundations* (University Park: Penn State University Press, 2010).

It is broadly accepted that privacy is contextually defined or articulated. That is, what is private in one setting or one era may not be so in other circumstances. A woman's body in the late stages of pregnancy, for instance, was considered private not long ago (at least if you were of the propertied class), as were knees, the state of one's mental health, one's efforts of conceive a child, various diseases such as alcoholism and epilepsy, the existence of illegitimate offspring, and so on. Privacy claims—or their legitimacy—also change with the setting or domain.[17]

Much of the dispute over the infamous Bill Clinton and Monica Lewinski affair concerned the question of whether being in public office cancelled one's right to a private life (and what one could and could not do in the oval office). Other types of jobs involve obvious forfeitures of privacy—the school bus driver must share his or her driving and criminal records, just as airline pilots must submit to the loss of privacy involved in drug and alcohol testing. Privacy claims also change with physical settings. The home is an obvious example of a domain in which what is private outside of it—such as one's bank account or health--may not be so inside. Likewise, a court of law can require that a person disclose details of his or her life that would normally be considered out of bounds.

Another way in which privacy is contextually relative concerns the issue of whom it is asserted against. Information which is private with regard to some persons, or groups of persons, is not with others. Our financial status, for instance, is well known to employees of the Internal Revenue Service or our banks, but not to our neighbors and casual acquaintances. This is precisely what is at stake with the Privacy Rules discussed—who we can validly say "It's none of your business" to and how we justify the boundaries we draw. Privacy, then, is asserted, protected, and defined in different ways depending upon the time and place as well as the people involved. Thus any account of the meaning and value of the concept must be context specific.

---

[17]As Schoeman describes it, "some social norms restrict access of others to an individual in a certain domain where the individual is accorded wide discretion concerning how to behave in this domain." (Schoeman, 1992), 15. Charles Fried characterizes the role of the setting by saying "Acts derive theirmeaning partly from their social context—from how many people know about them and what the knowledge consists of." *An Anatomy of Values: Problems of Personal and Social Choice*, (Cambridge: Harvard University Press, 1970), 137-154, 141.

The final general feature of privacy is that it is teleological concept. That is, privacy in and of itself is of little or no value; rather it's what it protects that matters.[18] It is for this reason that privacy is almost always defined in terms of other concepts such as liberty, dignity, personhood, intimacy and so on. Some theorists claim that privacy is in fact a cluster of concepts rather than a unified value.[19]

But for those of us who hold out hope for the concept as meaningful in itself, asking what *purpose* a claim to privacy is meant to serve enables us to at least narrow the range of values involved. What we need is a clear and specific way to differentiate between distinct versions, or perhaps different epochs, of the term "privacy." Only then can we judge whether the concept as commonly understood—if there is such an understanding—is coherent and up to the work expected of it.

In order to illustrate how these elements—domain, participants, and purpose[20]—are meant to help in identifying a particular understanding of privacy, let's look at a non-controversial example. Once we have a method with which to identify and evaluate claims to privacy, we can move on to the more difficult cases in dispute today. To begin with, however, perhaps the simplest and most longstanding use of the term "privacy" is in the context of the home.

---

[18] Whether "little" or "no" is the correct formulation is the subject of dispute amongst theorists. See for instance, Charles J. Friedrich's "Secrecy versus Privacy: The Democratic Dilemma," in Pennock, 1971. HHS states: "It is important not to lose sight of the *inherent* meaning of privacy: it speaks to our individual and collective freedom." (Preamble, at 9, emphasis added) Joseph Kupfer, on the other hand, holds that the concept occupies a sort of middle ground between instrumental and intrinsic value: "The view proposed here, then, sees privacy as more than contingently good but not quite valuable in itself." Joseph Kupfer, "Privacy, Autonomy, and Self-Concept," *American Philosophical Quarterly* 24 no. 1 (1987): 81-89. Perhaps the best discussion on this issue is in Fried, 1970: 137-8.

[19] Judith Jarvis Thomson, for instance, claims that "if, as I take it, every right in the right to privacy cluster is also in some other right cluster, there is no need to find the that-which-is-in-common to allrights in the right to privacy cluster and no need to settle disputes about its boundaries. For if I am right, the right to privacy is 'derivative'in this sense: it is possible to explain in the case of each right in the cluster how come we have it without ever once mentioning the right to privacy." "The Right to Privacy," *Philosophy and Public Affairs* 4 (1975): 295-314, 314. See also William Parent who claims that privacy is reducible to liberty claims in "A New Definition of Privacy for the Law," *Law and Philosophy* 2 (1983): 305-338.

[20] As mentioned, we can also differentiate accounts of privacy according to the era in which the privacy bid is made, but unless it is relevant (as it will be later), I shall simply assume we are talking about the present.

What do we mean when we say that the home is private? If there is anything constant about the meaning of a claim to privacy, it is that it includes the right of one party to block another, stopping the latter from intruding upon or learning of something in the former's life. With regard to the home, we are denoting a physical line—the front door or the beginning of our property (though this latter is debatable insofar as others are at least free to watch what we do in our front yards). Thus, the blocking involved concerns physical space. And that physical space is the setting for claims of privacy—that of the private domain.

(This may sound either circular or redundant, but as we shall see, not all settings or domains in which bids for privacy are made can be characterized simply in terms of the public/private distinction or even physical space; we can for instance, distinguish between the economic and the spiritual realms, or the political and the legal. These other kinds of domains will be of use when we get to more complex examples of privacy.) The participants of our simple example are fairly easily recognized as well—they include whoever lives in the home, on the one hand, and the rest of the world, on the other.(It's true that part of the latter group may switch sides if they are invited in, but not much rests on this so I shall ignore it for the time being.) If privacy is invoked, then, it will be by one of the inhabitants of the home against someone who does not have such status.

Finally, what purpose is served when the home dweller asserts his privacy? Obviously, there are myriad reasons why we might want to go home and close the door—we're tired, hungry, or just fed up; there are projects that we can do only, or best, there; it's the most propitious setting for relations with those we care about; or we simply have no where else we need to be. Any one of these might be operative at a given time, but we are looking for something more general, or perhaps universal. For our question is about *privacy*, not comfort, property, or relationships. These other values also clearly apply to home life, but they aren't the primary reason for demanding privacy. For instance, we might be able to be perfectly comfortable in a more public place, such as a youth hostel or a campground (admittedly, neither example brings to mind *great* comfort, but the point is that we can conceivably eat, rest, and sleep in non-private places).

The value that privacy of the home serves is more fundamental. The home is a sanctuary of sorts, where one needn't *be* anything. Being there relieves us of the requirements to follow the practices and rules involved in almost any other domain, such as the work place, the market place, or even just walking down the street. In all of these public domains, there are certain sorts of behaviors which are expected of us and others which are either prohibited or frowned upon. Wouldn't it be nice, for instance, to wear your slippers to work? Or leave your dishes on the table of the employee lounge until later when you felt like washing them? Or not talk? Or talk? Or sing off key? Or simply do nothing at all? This last example is especially illustrative of the value of privacy in the home; for there are few, if any, other places where one really can do nothing.

Even if we take a break in a park and just sit on the bench, we must still remember that we are in public—we don't usually lie on the bench or take our clothes off to be more comfortable (in fact, we could be arrested for either action).

It is only in the home—protected by a "zone of privacy," or what Michael Rowe calls "the outer envelope of personhood"[21]—that we are able to achieve utter freedom from conventions. As Hannah Arendt writes, "the four walls of one's private property offer the only reliable hiding place from the common public world, not only from everything that goes on in it but also from its very publicity, from being seen and being heard."[22]

It remains only to put a name on this value of freedom from social norms or publicity—the purpose of the privacy—though the label itself doesn't really matter. The important point is that it refers to a state which we seek, which is at times much needed if not absolutely necessary for us as human beings, and which we can recognize as important for others and therefore worthy of the protection. Nebulous though it sounds, I think it's something we all recognize, and it has been variously characterized in the literature as key in the development of a self-concept,[23] personhood,[24] inviolate personality,[25] and human dignity.[26]

---

[21] *Crossing Borders: Encounters between Homeless People and Outreach Workers* (Berkley: Univ. of California Press, 1999), 29. Rowe's discussion is concerned with physical privacy for the homeless, but the idea is the same—home and the privacy it affords are essential to human well-being.

[22] *The Human Condition* (University of Chicago Press, 1958), 71.

[23] Kupfer, 1987, 81. "A Concept of self as empowered to determine one's life, it will be argued, is requisite to *acting* autonomously. And privacy is needed for such a self-concept to develop."

[24] Jeffrey Reiman, "Privacy, Intimacy, and Personhood," *Philosophy and Public Affairs* 5 (1976): 26-44, 39. "*Privacy is a social ritual by means of which an individual's moral title to his existence is conferred.* Privacy is an

The idea, in other words, is that unless we can get out of the public view now and then, we are potentially forever a slave to the opinion of others. (In this context, it is worth comparing life in prison, or other sorts of so-called total institutions, with the sort of respite we seek in the home.) Privacy in the home allows us to take a break from the rules and the pressures of such opinion, to refresh ourselves, and hopefully, to determine for ourselves whowe are in relation to that public.

Thus, the purpose of asserting the privacy of our home is not simply so that we may wear our slippers or sing off key. Rather it is that having the space and time in which to behave in such ways also serves a greater end—that of figuring out who we are and how we want to live.

It is for this reason that privacy is cashed out in terms of the other important values—dignity, respect, personhood—rather than the more specific freedom to eat, dress, or sing in any particular way.

As a final means of illustrating the three different elements of privacy claims (domain, participants, and purpose) and the usefulness in spelling them, consider the privacy one might claim for financial records. For instance, why is it that banks that publish their customers' account statements in the local newspaper would rightfully be accused of violating the privacy of those clients? Again, the participants and domaincan be quickly disposed of. The first include the bank's employees and/or owners as well as the customers. The relevant domain might be described as the business (or financial) domain. (Note that the point of specifying the domain is to make explicit the duties, obligations, expectations, and rights which apply to one type of interaction but not others. Thus the label itself is not as important as what is implied by it—in this case a fiduciary relationship, incurring obligations of trust and confidentiality.)

---

essential part of the complex social practice by means of which the social group recognizes—and communicates to the individual—that his existence is his own."

[25] Warren and Brandeis, in Schoeman, 1984, 82.

[26] Edward J. Bloustein, "Privacy as an Aspect of Human Dignity: an Answer to Dean Prosser" in Schoeman, 156-202. "The man who is compelled to live every minute of his life among others and whose every need, thought, desire, fancy, or gratification is subject to public scrutiny, has been deprived of his individuality and his human dignity."

What purpose is served by demanding privacy in this realm, or by crying foul play when such privacy is blatantly violated? In other words, why do we *not* want our financial status to be public knowledge? As in the case of privacy in the home, there may be any number of quite specific reasons we don't want others to know our bank balance—we might be afraid they will hit us up for a loan; that they won't want to travel with us; or that they might begin to monitor our expenditures. Irritating though all these might be, the grander purpose, so to speak, is that in order to be in control of our own lives, we need to be able to filter the information other people have about us. Although we can't do this with all personal information, when at all possible, we want to be able to choose what others may know, realizing as we all do that people react differently based on the sort of information they possess.

Imagine we repeatedly go to happy hour together, and I never have enough money to pay for my share of the drinks. If you are a generous sort and believe that I am struggling financially, you may well be perfectly happy to cover the tab if you enjoy my company sufficiently. If, however, you were to find out that I have plenty of money and am simply cheap, your attitude would likely be very different no matter how much (you thought) you enjoyed my company.

The reasons we value the privacy of our banking records and other financial information, then, are quite different than those which we identified in the context of the home. In particular, our purpose in demanding privacy of such records primarily concerns our relationship with others, rather than our own state of mind or independent development. Privacy as a means of regulating what others may know about us—that which is involved in the banking case—is often characterized as self-determination or autonomy insofar as it allows us (to the extent possible) to be the authors of our own life, to have the persona we wish the world to see out there.

As we have seen, the value and meaning of privacy is goal-specific. For if there is any inherent meaning to the concept at all, it is simply a form of blocking, of keeping others out, whether it be from a physical space, or possessing certain sorts of information, or of preventing action of a particular sort (as with obtaining an abortion). But blocking *alone* does not constitute privacy—road blocks aren't claims to privacy, nor are baby gates or minimum age requirements for entering bars. In order to be an instance of bid for privacy, it must be done for a particular purpose.

What confuses us about the term is that while not all purposes pursued in blocking constitute privacy demands, neither is it the case that such demands can be captured under a single type of purpose. Privacy is, perhaps uniquely, complex. For it is used—and used correctly—in utterly disparate ways, and yet remains a single concept, albeit one which is in dispute.

Privacy Updated

The argument of the previous section was that in order to understand, and evaluate, a bid for privacy we must look to the context in which it is asserted, including the domain and the participants. But we must also identify the purpose of the protection demanded, not to define the concept, but rather to evaluate whether it is indeed a genuine bid for privacy or for something else altogether.

Once again, privacy is a notoriously slippery term, leading to authors like Laurence Tribe to describe (but not adopt) views held by "those who regard privacy as but a name for a grab-bag of unrelated goodies."[27] It is also described as a "cluster of concepts" or one which has a "multi-dimensional form."

Despite these disagreements in taxonomy, however, it is broadly agreed upon, in the philosophical and legal literature at least, that the term (and its progeny) is essentially normative. That is, privacy is something worth demanding because it is intimately related to value concepts like intimacy, autonomy, personhood, liberty, integrity, trust, human dignity, and identity. Privacy is worthwhile because it enablesus to achieve these goods. Whether it be about information about, surveillance of, or intrusion on what is exclusively ours, we become unable to control our very identity in the eyes of others, thus losing autonomy at minimum, and frequently dignity and the rest as well. As Warren and Brandeis say in the classic article on the right privacy, it involves an individual's "right of determining, ordinarily, to what extent his thoughts, sentiments, and emotions shall be communicated to others." And when that right is violated, he loses "the right to one's personality."[28] Privacy is intrinsically normative and teleological.

---

[27] Quoted in DeCew, 1997, 62.

[28] "The Right to Privacy," *Harvard Law Review* 4 no. 5 (1890): 193-220, 198, 205.

In order to evaluate the validity of the claims to protect privacy discussed in Part One, then, we need to identify the domain, participants, and purposes of the Rules. The analysis will focus on the protection of medical records, but much the same goes for the financial version given the similarities in structure. The Preamble of the Final Privacy Rule states that:"the provision of high-quality health care requires the exchange of personal, often-sensitive (sic) information between an individual and a skilled practitioner. Vital to that interaction is the patient's ability to trust that the information shared will be protected and kept confidential. Yet many patients are concerned that their information is not protected."[29]

In response to such concerns, polls were taken and evaluated, congressional representatives contacted and consulted, and the industries involved (including the insurance companies) were called upon to take the steps necessary to reassure the American public that medical records were indeed responsibly handled.

The Final Rule was over five hundred pages (with commentary), and is of such complexity that it took years to fully implement and required large scale restructuring of almost all aspects of health care. Protection took effort. Up until the early to mid-1960's, concern for privacy roughly followed the Warren and Brandeis model of 1890.

That is, rights to privacy were generally considered to be justified claims preventing others from intruding upon the inner sanctum—the domestic realm. Words like "solitude," "seclusion," and "retreat" were far more likely to appear in discussions of privacy than those which are frequently touted today, such as "security," "control," and "efficiency." For in its infancy, what was protected was naturally located predominantly in the home. The concern was that "what is whispered in the closet shall be proclaimed from the house-tops."[30]

Today, of course, whispers are the least of our problems. As pointed out by the ACLU's John H. F. Shattuck, "record-keeping is one of man's oldest activities. In this perspective, computerization of personal records represents the latest stage in a procession of techniques that has developed over the past 4000 years from clay tablet, and papyrus scroll to typewriter, teletype and Xerox copier…"[31]

---

[29] Federal Register: December 28, 2000 (Volume 65, Number 250): 8.
[30] Judge Cooley, qtd. in Warren and Brandeis, 195.
[31] *Rights of Privacy* (Boston: National Textbook Company, 1977), 149.

Thus, there have always been records and documents "out there," some of which were probably regretted by the subject.

Despite its long history, though, we have obviously made a quantum leap today, rather than the incremental development of new kinds of record keeping described. The change in focus from keeping others from intruding upon the home to protecting information held outside the home, in other words, wasn't simply a result humans' sudden propensity to keep records. Rather it was the format of the records, as well as the radically increased pace, size, and complexity of the public realm generally, and the world of business specifically, which led to worries going far beyond intrusion upon the domestic sphere. It is here where the difference in era or time comes in. Marx and Engels' description of the enormity of the changes wrought by the rise of the bourgeoisie might well be an (possibly overly dramatic) account of the effects of digital record keeping:

> Constant revolutionising of production, uninterrupted disturbance of all social conditions, everlasting uncertainty and agitation distinguish the bourgeois epoch from all earlier ones. All fixed, fast, frozen relations, with their train of ancient and venerable prejudices and opinions, are swept away, all new formed ones become antiquated before they can ossify. All that is solid melts into air.[32]

Moreover, rather than protecting a man's "thoughts, sentiments, and emotions" as Brandeis and Warren put it, privacy would now be directed at man's financial, medical, and criminal histories. With the computer—the so-called age of access—the stakes go up. There will still be concern for the private realm as the Court's decision in Kyllo v. U.S. shows—a man's house is still his castle.[33] But just as the processes described by Marx and Engels have never been reversed, changes in what it takes to manage and control one's own business will never be the same. As HHS states in the Preamble of the Final Privacy Rule, "Today, it is virtually impossible for any person to be truly 'let alone.'"[34]

---

[32] *Manifesto of the Communist Party*. *The Portable Marx.* Eugene Kamenka, ed. (NY: Penguin, 1983).

[33] 533 U.S. 27 (2001). The plaintiff was arrested for growing marijuana in his home as a result of the use of thermal imaging by the police outside of the home. While the defendants claimed they were within their rights since they never entered the residence, the Court found that the surveillance did in fact violate the 4th amendment's promise of freedom from arbitrary search.

[34] Preamble, 11.

So what is the context of the bid for privacy in the medical records case? Who are the participants and what are the domain and purpose? It is by answering these questions that we see the need to reconsider our understanding of privacy (and the possibility of attaining it) given radically changed circumstances. For the context has changed beyond recognition. Just as Marx and Engels explain the very conditions of society through the revolutionary developments of successive epochs, we find ourselves in a world we could not have imagined fifty years ago. Our very concepts of space and time have expanded through the invention of the computer and the internet. Concrete spatial boundaries are almost secondary; records which could once be confined to one or two physical locations are now "out there" to such a degree that reining them in again seems virtually impossible.[35]

Concurrently, the number of participants handling those records has grown exponentially. We are clearly not in Kansas anymore. The question is, can we still have genuine *privacy*, or is the best we can do something else?

Compare current practices regarding medical records with those of a physician practicing in 1920. In the earlier era, the records would usually be hand-written, contained within a single folder, and kept in a single office. Access to the records would be available to the physician who originated them, his or her partners, and the nursing and perhaps, administrative staff. In many cases, this may well have amounted to only one or two people. Contrast this with today's scenario in which any number of people need (and get) access to medical records and, given the format, get it quite easily.

As reported by HHS, "according to the American Health Information Management Association (AHIMA), an average of 150 people 'from nursing staff to x-ray technicians, to billing clerks' have access to a patient's medical records during the course of a typical hospitalization."[36] Even apart from hospital stays, the privacy legislation (which is after all meant to *limit* access to patients' personal health information) roughly says that anyone who is in the business of the provision, payment, and health care operations has carte blanche.

---

35 Marx and Engels' words are also apt here when they describe the rise of the bourgeoisie as creating "a society that has conjured up such gigantic means of production and exchange, [it] is like the sorcerer who is no longer able to control the powers of the nether world whom he has called up by his spells." (*Manifesto*.)

36 Final Privacy Rule – Background and Purpose, 14.

(Note that that same is true in the financial privacy rule—any affiliate of the financial institution may have access to information without consent or notification.)

Even a single office visit can generate *legitimate and necessary* access to all those listed under "health care operations" as well as those involved in the actual payment procedure, never mind those that actually deliver the care. While it is obvious that the entire system is top-heavy, that is not our immediate concern. Before the computer age, the physician and staff would have to have some system of record keeping whereby files and notes were shared, but only for purposes directly related to care. As far as anyone else was concerned, old-fashioned manila folders and file cabinets usually did the trick.

Moreover, the staff would have to be committed to maintaining confidentiality in other ways, such as refraining from talking about particular cases outside of the office, or reporting to the newspapers when a celebrity came for health care. Apart from that, however, there seems little else which would be required of the physician and his or her staff. In other words, maintaining privacy would have been largely a matter or *refraining* from disclosing the information in wrongful ways (and given the system of care, almost all forms of disclosure outside of the office would be considered wrongful). In such a case, the right to privacy was a *negative right,* one which required only that those on the other side, so to speak—those who have the duties correlated to the right—refrain from certain behaviors. The right required no positive action on their part, and as such, was significantly easier to honor.

In contemporary times, on the other hand, to respect the right to privacy one will have to do a good deal more. For simply refraining from disclosing the information simply isn't possible.

Disclosure is a normal, and required, part of the job and occurs whenever the provider seeks payment or authorization for a procedure, gives the patient a referral, or submits reports to the HMO under which he or she operates (to name just a few transactions). The information is already "out there," usually in a format which is easily and instantaneously shared, and unless one is very young indeed, simply a further chapter to an already existing file. Protecting privacy under these circumstances is far more difficult than in the earlier case.

Not only is it a more complicated matter, one which involves more complex judgments of legitimacy, wrongful use, and so on, but it is going to require positive action on the part of those who deal with such information—a group which is vastly increased. The right to privacy has, in other words, turned into a *positive right*, one which requires that those who hold the duties correlated do much more than simply stand out of the way. At minimum one will have to think about the security of transmission as well as procedures by which to store and dispose of the information. A burglary of physical records in the physician's office is easily detected; hackers present more of a challenge.

Interestingly, the purpose served by protecting privacy seems to have roughly remained the same in the two eras. Personal medical information is sensitive; the mode and scope of the health care system do not change this fact. Given this sensitivity, individuals might be reluctant to share it. We might explain this tendency in privacy terms as the desire to be the authors of our public persona. As previously discussed, what people know about us can easily change the way they feel and think about us, treat us, and judge us. Disclosing that an adult is HIV positive is practically equivalent to disclosing that he or she has had some sort of sexual interaction or is in intravenous drug user (or has been extremely unlucky with hospital care). And those disclosures may well affect that person's job prospects, housing options, dental treatment, number of suitors, and general standing in the community. This is not to endorse discrimination against AIDS patients, but merely to point out the way in which disclosing medical information can radically change a person's situation—usually for the worse.

However, if a patient is unwilling to fully disclose medical details to his or her physician, the quality of medical care may well go down. HHS elaborates: "privacy is a necessary foundation for delivery of high quality health care.

In short, the entire health care system is built upon the willingness of individuals to share the most intimate details of their livers with their health care providers.[37] Again, this necessity has not changed as the context and number of participants involved have. Control over medical (or financial) records remains important insofar as we wish to regulate what others may know about us, realizing that certain kinds of information can radically alter their treatment and judgments of us.

---

[37] Preamble, 16.

In summary, by working with a contextually articulated approach to privacy we have seen first that the domain in which such privacy is asserted is transformed beyond recognition. What was spatially delineated is no longer describable in terms of geography. Not only must we contend with cyberspace and the immediacy and breadth of information sharing it implies, but the great number of participants involved in the delivery of health care—including insurers, pharmacists, accountants, health care clearinghouses, doctors, nurses, technicians, employers, and others—makes thinking of a single geographical designation for the bid to privacy utterly obsolete.

This last point illustrates the fact that the change in domain is intimately related to the change in participants which is unsurprising. The domain represents the setting in which the claim to privacy is made; if that setting has been greatly expanded, it only makes sense that the number of participants would expand as well. What is not so immediately clear is how the purpose of the privacy claim interacts with the context in which it is made, a point I will return to presently.

Continuing with the summary of findings to date, we have seen that while the purpose for demanding privacy remains the same, the way in which that purpose is realizable is radically quite different. For given the contextual changes, the right to privacy must now be asserted against countless, unknown individuals rather than a specifiable few. Moreover, as mentioned in connection with the distinction between positive and negative rights, the contemporary right to control one's own private information requires far more of those who have it than simply restraint. For many of the participants, disclosure is what they *do*. The whole point of health care clearing houses is to reformat information (from identifiable to non-identifiable, but also vice versa) and *pass it along*. Likewise for financial supermarkets. Thus rather than simply demanding that those who have access to sensitive information keep it confidential, we must specify how, when, and to whom they may disclose it. And this, of course, is far more complicated.

HIPPAA requires that there be "Privacy Officers" with varying degrees of access, necessitating both special training and positive rules to prevent access. So much more is required from those against whom the demand for privacy is made—keeping information confidential is an enormous (and costly) job. The duties correlated with a contemporary right to medical or financial privacy are substantial.

What should we conclude from these findings? First, as already mentioned, it looks as though changes in domain and changes in participants will be likely to go hand in hand—the context is a package deal. The more interesting finding, however, is the relation between that context, the purpose of the privacy bid, and its value in relation to other values. In the case of informational privacy, it seems to cash out this way. The change in context—domain, era, and participants—radically changes the very possibility of achieving the end of privacy in the sense of controlling what others may know of us (the purpose).

While our reason for wanting privacy of medical and financial records may have remained the same over time, the possibility of getting it has not. We may get data security, predictability, and accountability, but we simply do not have the option of *controlling*, in any meaningful way, who sees our personal information.

The purpose of the claim to privacy prior to electronic records and the vast business that goes with them, was perhaps most importantly to guard our dignity—the body is subject to all sorts of unlovely conditions we may be unwilling to share. But the privacy claim is also about maintaining our autonomy by controlling what others may know about us. Likewise with identity (consider operations like abortion, breast enhancement, or sex reassignment surgery) and one's future decisions regarding intimacy. However—and this is the punch line—these moral goods are no longer possible in any substantive way. Not only are there countless unknown people who "know" (though probably don't care), but anyone we see in the profession today will likely know our history regardless of relevance to present complaints. The cat is out of the bag and very unlikely to be in it ever again. Warren and Brandeis' concern over "whispers in the closet" are well-founded.That records are shared needn't mean that we will in fact have lost dignity or autonomy, but these terms are simply not apt for what the Rules were built to do.

Rather than the normative goals which have been an inherent part of the right privacy against society at large, the ends we seek today are empirical—security, regulation, standardization, consistency, and so on. Even when accomplished it is not privacy in any meaningful sense which is secured. This conclusion may be disappointing, but it is important to remember that just because we cannot have privacy, it doesn't follow that anything goes.

Data security and accountability on the part of those who handle our information are clearly attainable and may well be an adequate replacement for the spot previously held by the normative concept of privacy (even if it is still so-called). Given radical changes in domain and participants—changes which are unlikely to be reversed—our goals themselves have necessarily changed as well. Substantive privacy is still possible, just not in the context of extensive sharing of incalculably many bits of personal information—in other words, not in the context of current medical and financial transactions. What we need in those contexts has been transformed; the purpose of the Rules is security and so on, not protection of our "inviolate personality."[38]

Moreover, whether or not we like the conclusion is irrelevant. If the argument presented here is correct, privacy in the sense of genuinely controlling dissemination of our personal information is simply no longer possible. We can inform ourselves on the conduits of distribution, keep a close eye on our physicians and financiers, take the time to find and opt-out of whatever systems we can, or even refuse to have dealings with anyone who uses a computer for official business. Absent these, however, there is little we can do to completely hold on to what is ours. What we can do, however, is to stop thinking that it is privacy which is protected and then getting disappointed when it is not. Legislation like the Rules threaten the very meaning and value of privacy in other realms in which it is still possible. For they give us false hope that privacy will be protected, and that hope is inevitably dashed. If this happens frequently enough "privacy protection" will no longer kindle hope much less confidence; and its fundamental value in relation to our very personhood may be lost. The HHS's statement in the Preamble of the HIPPAA Rule that "today, it is virtually impossible for any person to be truly 'let alone'" should concern us not so much because it is true that we will be known in some way to many. Rather we should find it very disconcerting that in using the central description of privacy—the right to be left alone—it states that we have lost privacy for good.

---

[38] Warren and Brandeis, "The Right to Privacy." 205.

Conclusion: Back to Snowden

So what does this tell us about the Snowden affair? The revelations that the NSA has secretly been gathering enormous amounts of information about Americans and foreigners from emails, credit card transactions, phone calls, internet searches and so on is creepy to say the very least.[39] The degree to which individuals' private information has been gathered and with whom it has been shared is as yet unknown (though the government has assured the public that it only looks at the suspicious stuff—not exactly the comfort we seek).

While immediate action should take place in response to a dragnet of questionable legitimacy, it is not yet possible to do much by way of theoretical analysis of the effect on the rights of individuals. However, what we have learned about medical and financial records and the attempts to keep them "private" might help. For we know that it is not normatively-based privacy that we can demand (though it will no doubt be continued to be called it), but rather accountability, transparency, necessity, and predictability. While we cannot say how these concepts should be applied exactly, we do know that we want them to applied and that if they are not, we are indeed losing something of great importance. But again, it is not the "inviolate personality," the absolute "right to be let alone," or the "outer envelopes of our persons." This needn't mean that what has been invaded is not fundamentally important; but it does mean that it is different. We should, then, be looking for different solutions—those of regulation and control rather than autonomy and freedom.

---

39 The surveillance is technically authorized only on foreign "suspects" based on the Foreign Intelligence Surveillance Court (FISA) created in 1978. After the creation of PATRIOT Act in 2001 (reauthorized in 2005) the scope of surveillance broadened exponentially under the authority Section 215 which allows for secret requests for authorization of information gathering. The scope of the searches has also broadened as a result of electronic contacts between US citizens and foreigners, or even a US citizen's internet search regarding foreigners. Finally, the language governing what is a reasonable source of suspicion has been weakened substantially to anything which is "relevant to terrorism."