Toward an Institution-based Theory of Privacy

Lee Wilkins, Philip Patterson

Published online on: 31 Mar 2020

How to cite:
In the twenty-first century—an era dominated by U.S.-based information and entertainment conglomerates—law, ethics and technology intersect over the issue of privacy in far reaching and sometimes confusing ways. This chapter acknowledges that while thinking about the notion of privacy emerges from philosophy, this philosophical thinking has been applied through the creation of law and other documents that carry the force of law to form the current notion of a “right to privacy.” In working toward an institution-based theory of privacy, this chapter begins by accepting that, when it comes to clear thinking about privacy, law and ethics must be connected. It rejects Immanuel Kant’s assertion that law and ethics are “two distinct and non-intersecting” intellectual responses to human problems, a stance also supported by more contemporary thinkers (Fletcher, 1987). And, while some scholars have sought to make this connection through the work of Jürgen Habermas, as reviewed by Glasser and Weiland in this Handbook, this chapter employs feminist epistemology (Koehn, 1998)—allowing ethics issues to emerge from authentic life experiences—to connect both law and ethics to the role that technology now plays in how people, and the machines that they program and control, consider privacy. By triangulating the “issue” of privacy in this way, this effort also calls for additional theorizing about how privacy might be defined and how people in their intersecting roles as citizens, consumers and media practitioners should think about the concept. It also takes a first step in that theoretical direction.

But, to begin, the chapter reviews how philosophy and ethics provide a basis for the law of privacy and a way of both understanding and critiquing the law. The origin of the word “philosophy”—a love of knowing—foreshadows the fact that deciding “who should know what and when,” (in other words the components of privacy) are deeply rooted in philosophy.

PRIVACY: THE PHILOSOPHICAL ROOTS

Thinking about privacy began with the Greeks and has focused on two understandings about human beings and community that are not only more than 3,000 years old but also as current as Facebook content. The Greeks wrote that the concept of privacy was rooted in information about the individual. It was among the elements of human dignity and autonomy as initially defined in the Greek philosophical tradition. They also linked privacy to the context in which
that information is understood—the term context meaning a tightly constrained circle of human beings who are aware of the information. Context implies human beings living in a community, and that element of community is important when thinking about privacy in this 21st century. We will return to it after some additional concepts are clarified.

To begin, there is a distinction between privacy and secrecy: secrets are known by a single person only, private information is tightly held among a specific human and intimate circle. Philosopher Sissela Bok (1983, pp. 10–11) defined privacy as “the condition of being protected from unwanted access by others—either physical access, personal information or attention.” Judge Alan Westin (1967) calls privacy “the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others” (p. 7).

Perhaps this example will help clarify the distinction. Dreams are secret—they are known only to the dreamer. A rape is private—it is known to at least two people: the rapist and the victim. In contemporary cultures, many hope that a rape is also known to the police or other law enforcement authorities, to the doctors and other medical personnel who treated the victim, and to the victim’s loved ones, who may be helping the victim recover physically and psychologically. But, with this particular crime, that is where the “knowing” should stop. The rape should not be known to the cashier at the grocery store who recognizes the name on a debit card because the cashier saw a report of the story on a local television newscast or received a tweet about the story from a friend.

Expanding on the work of Bok, people do not need to demand secrecy in order to desire privacy. In the case of Dietemann v. Time Inc. (449 F. 2d245) (1971), Judge Alan Westin awarded damages to a man (Dietemann) whose privacy had been invaded by investigative reporters for Life magazine. Westin said: “The claim is not so much one of total secrecy as it is of the right to define one’s circle of intimacy—to choose who shall see beneath the quotidian mask.”

The visual image of “circles of intimacy” illustrates the concept. Imagine standing at the center of a series of concentric circles of intimacy in which your relationships get more distant as the circle radiates out and gets larger. In the center is just you—your fantasies, hopes, memories—some articulated, some not. You can choose to share these thoughts or keep them to yourself. The choice is yours—something that was taken away in George Orwell’s novel, 1984, or in the contemporary novels and films based on The Hunger Games trilogy.

In the second circle are you and another person of your choosing. It could be a spouse, sometimes a professional, such as a member of the clergy, a lawyer, a roommate, a doctor, or a college counselor. In fact, most people have multiple “you + 1 circles” going simultaneously and for different reasons. In this second circle you share intimacies that you want only the one other person to know; the context in which these intimacies are shared is also an intimate one. The relationship rests on trust, trust that a confidante will neither betray the trust nor use the revelation to your disadvantage. U.S. law recognizes the importance of these primary relationships.

The third circle includes others—family, roommates, close friends, teammates, and so forth. People in this circle know things about you that you would not want to be “public” knowledge. Reciprocity forms the glue that holds this circle together. Again, the key moral ingredient is control over who does and does not get access to private information and the assurance that those who do have access also have the deep knowledge with which to interpret it.

As the circles enlarge, the numbers of potential confidants gets larger and control over the information decreases. The image extends to the outermost imaginable circle—all humanity. There are some things about yourself that you would not object to all humanity knowing. Those things constitute your most “public” self. Various U.S. laws recognize this outer circle such as the “directory information” exclusion in FERPA laws that govern strict privacy in educational
In modern society, as people willingly disgorge increasing amounts of information in digital spaces such as Facebook, we lose control of our circles of intimacy. Items once at the core of our being are now flung to the fringes for the world to see. In the Dietemann case, Dietemann welcomed reporters into his home under false premises. When his solitude was disrupted by the resulting story (it was about medical quackery, and Dietemann was implicated), neither the story’s veracity nor its social importance could “redeem” the lies told by the reporters to get the story.

Thinking about privacy philosophically has prompted scholars to develop four different types of potential harms when privacy is invaded (Nissenbaum, 2008): informational harm (such as identity theft), informational inequality, (such as governments and corporations amassing large amounts of data about individuals without their knowledge or consent), informational injustice (for example, transferring data from your financial records to the local newspaper without appropriate contextual information) and encroachment on moral autonomy, “the capacity to shape our own moral biographies, to reflect on our moral careers, to evaluate and identify with our own moral choices, without the critical gaze and interference of others” including pressures to conform to social norms (van den Hoven, 2008, p. 439). Three of these harms implicate powerful institutions and technology, something that philosophy with its focus on individual autonomy and accountability, historically has addressed only incompletely.

The Role of Discretion

Returning to the previous example of rape reporting, an additional concept about privacy emerges from the philosophical tradition: discretion. Discretion is the ability to understand, on a moral basis, why some information should be shared and some information withheld. Discretion is a process of evaluating the harm that information may and may not do when shared and then making a rational choice about sharing it. Discretion does not mean never sharing information; it means knowing when to share, with whom, and under what circumstances withholding information produces the least harm to all involved. In philosophy, discretion assumes a human actor and human-based decision-making.

In contemporary American journalism, journalists often know the names of rape victims but withhold that information from their viewers/listeners/readers so as not to reinjure a person who has already been injured by the rape. By exercising discretion, the journalist ensures the victim has control over those who know about the crime and its impact on the victim. Perhaps the victim decides to confide in a larger public, as was the case in a newspaper story which won the 1991 Pulitzer Prize in Public Service by reporter Jane Schorer and editor Geneva Overholser of the Des Moines Register. The poignant story revealed the name of a rape victim willingly discussing the ordeal a woman faces when deciding to press charges over such a violent assault. Even in this instance, the victim retained control over sharing the information.

In the case of the Boston Globe’s (2002) reporting of the pedophile priest scandal in the first decade of this century (reporting which was summarized in the Oscar-winning film “Spotlight” in 2015), discretion included withholding the victims’ names, but not the nature of the assaults themselves. Discretion is most certainly context dependent, and context implies community. “A credible ethics of privacy needs to be rooted in the common good rather than individual rights” (Christians, 2010). “Communitarians see the myth of the self-contained ‘man’ in a state of nature as politically misleading and dangerous.”

The Globe’s reporting is an affirming example of the nature of privacy and discretion as articulated by journalists. The community of Boston and the worldwide community of Roman
Catholics needed to know of this cancer within the Catholic clergy. Knowing was the common good. Maintaining community meant revealing the nature of the crimes committed, despite the harm that it would do to the institution, so that the community could continue to live with autonomy and dignity and the institution itself might improve.

While we most often think of discretion as an individual decision, and learning to exercise discretion as one of the markers of a morally-developed person, in this century discretion most often involves third parties to whom we willingly—and sometimes not—give information. People willingly disclose personal information about finances, health, and even chromosomal makeup to obtain mortgages or medical diagnoses. The assumption is that the mortgage broker does not acquire a client’s medical records and the doctor will not acquire financial information.

Some contextual boundaries will continue to exist. But, one of the results of Wikileaks and the reporting based on Edward Snowden’s revelations is the grudging acknowledgement that governments spy on citizens and on one another, sometimes by jawboning communication conglomerates to turn over access to individual telephone records and by analyzing the content of that communication. These revelations have become one of the most notorious examples of the use of “big data” for the stated purpose of improving national (and hence individual) security without ever requesting permission from the citizenry or its elected representatives.

With “data mining” the new financial and espionage frontier, what ought to be the rules of third-party, institutional discretion? Historically, Americans have refused to accept that a “third party”—beginning with government but extending to some private, for-profit institutions—would be able to exercise discretion without substantial guidance. Law constrained such acts, and it was to the law—the world of rights—that thinking about privacy turned.

Finding a New Right

The genesis of the term “Right to Privacy” comes from an 1890 Harvard Law Review article authored by Louis Brandeis (later a Supreme Court Associate Justice) and Samuel Warren. Though several historical “versions” of the story exist, the most common one is that the two influential Boston lawyers were incensed by unwanted media coverage of the marriage of Warren’s daughter during the era of “yellow journalism.” Little has changed in the subsequent 125 years since one of the most influential law review articles of all time was written. In it, Warren and Brandeis (1890) argued for the right of the individual to be free from the snooping eyes of the press. Today, thanks to the work of Dean William Prosser, the tort of privacy has four legally-recognized manifestations:

1. Intrusion upon a person’s seclusion or solitude, such as invading one’s home or personal papers to get a story—philosophically, a loss of control over information;
2. Public disclosure of embarrassing private facts, such as revealing someone’s notorious past when it has no bearing on that person’s present status—another example of loss of control over information;
3. Publicity that places a person in a false light, such as enhancing a subject’s biography to sell additional books—an inappropriate shifting of the context in which information is understood;
4. Misappropriation of a person’s name or likeness for personal advantage—another assault on information context.

Despite the legal history that informs the concept, the “right to privacy” never appears in the U.S. Constitution. In an early, seminal case in privacy law, Griswold v. Connecticut, Justice William O. Douglas made the argument that the matter of a “right to privacy” is addressed in the
“penumbra of the US Constitution.” This term, penumbra, used nearly a dozen times in Supreme Court decisions, always refers to rights that can be inferred by other rights. So, the right to privacy is found in the totality of rights enumerated in the Bill of Rights.

While this is the basis of privacy in U.S. law—a right that is inferred rather than explicitly stated—the Universal Declaration of Human Rights, which was written almost 200 years after the Bill of Rights to the U.S. Constitution was approved, explicitly names privacy as a right of all people, regardless of citizenship. What constitutes that “right” is left undefined.

The distinction between a right that is inferred as compared to one that is explicitly articulated is important. In the U.S., privacy has evolved as a right conferred by the courts, based in law, while in the rest of the world it is a human right, what the American Founders would have called a “natural right.” Jefferson noted three such natural rights in the Declaration of Independence: life, liberty and the pursuit of happiness. The first two Jefferson borrowed from Locke; the latter comes from Aristotle. The “bottom line” of the Declaration of Independence is that natural rights need no justification—they simply are beyond debate. For most of the world, privacy is a natural right, while in the U.S., the right continues to be about law, although by linking natural rights to “happiness” or what the Greeks called “flourishing”, the argument that philosophy informs the law of privacy, even in the U.S., has substantial intellectual merit.

Interestingly, in the last half of the twentieth century, virtually every major court case that has carved out the U.S. notion of a right to privacy was a case over sexual matters such as contraception (Griswold v. Connecticut), abortion (Roe v. Wade) and sodomy (Bowers v. Hardwick). One at a time, as these cases were granted writ by the Supreme Court against long odds and invariably found in favor of plaintiffs seeking relief from state intrusion into their lives, a larger notion of privacy was created out of the most intimate of decisions a person could make. The progression is instructive: the further from the center of my circles of intimacy an event occurs, the less control I have over what is made public. In the U.S., the balance between community and the individual tilted toward the individual and to individual rights.

However, when the issue is privacy, the community and the individual have a symbiotic arrangement—one is not possible without the other. As western law sees it, privacy is an a priori right, meaning a right that can be justifiably overwhelmed by other concerns. Those concerns are most often stated in terms of the needs of the larger community: the Boston Globe’s reporting provides a robust example of how philosophy and law inform one another over the issue.

Philosopher Louis Hodges notes a fundamental “need for privacy” saying that “without some degree of privacy, civilized life would be impossible” (Glasser, 1983). Hodges says that individuals need privacy to “try out” new poses and new selves without fear of ridicule. He also argues that communities of individuals need privacy as a shield against the power of the state that might otherwise coerce individuals in a variety of ways for a variety of ends.

Communally, privacy is a necessary component of a democracy—without community an individual is unable to know himself in relation to others and the individual is also unable to govern herself—a process that must involve cooperation, collaboration and sometimes conflict with others. Governing demands mature citizens learning what information to guard, what information to reveal and for which ends.

This tension between community and individual privacy has been part of Jewish religious teachings for more than two millennia.

Avoiding the “Unwanted Gaze”

Unlike the harm of libel, which requires “publication” in writing or orally, invasion of privacy sometimes involves no publication at all. And, indeed the harm from intrusion on one’s solitude might actually occur prior to publication or dissemination not because of it. In his book The
Unwanted Gaze, legal scholar Jeffrey Rosen (2000, p. 18) notes that Jewish law as codified in the Talmud has developed “a remarkable body of doctrine around the concept of hezzek re’iyyah,” which means “the injury caused by seeing” or “the injury caused by being seen.”

According to Rosen, this doctrine expands the right of privacy to protect individuals not only from physical intrusions into the home but also from surveillance by a neighbor who is outside the home, perhaps peering through a window into a common courtyard. Jewish law protects neighbors not only from unwanted observation, but also from the possibility of being observed. The law is detailed and strict. If your window looks into your neighbor’s private courtyard, you must seal your window shut. “From its earliest days, Jewish law has recognized that it is the uncertainty about whether or not we are being observed that forces us to lead more constricted lives and inhibits us from speaking and acting freely in public” (Rosen, 2000, p. 19).

That sentence is important: fear of being observed causes us to partially shut down our lives where we are celebrating, mourning or just going about a daily pattern. Again, it calls to mind the notion of trying out one’s “poses” and possible “future selves” as a reason for the “need for privacy.” If the courtyard represents information that is available to individuals living in community, then knowing when to “avert your eyes” requires choosing among alternatives. Ethical thinking divides information into three, unequal and not always overlapping, categories: “want to know,” “need to know” and “right to know” and places the responsibility for knowing the difference on the individual doing the “seeing.”

“Want to know” information abounds and entire media and mediums exist to serve it. Wanting to be involved in others’ lives explains the reason for and the content of social media such as Facebook or Instagram as well as the tabloid press and reality television. The entire international culture of celebrity is based on the public’s almost insatiable appetite for information about their favorite heroes from sports, film, music, royalty, and so forth. Carol Burnett, a famous comedienne of the last century who successfully sued the U.S. tabloid newspaper the National Enquirer for libel, told an interviewer: “A public figure has little in the way of private life. That’s a fact of life for those involved in careers that increase public visibility; with increased visibility comes natural curiosity to know more about the person” (Burnett, 1983).

However, curiosity does not make a compelling philosophical claim, despite that fact that the economic logic is something many media corporations find compelling. Curiosity does not serve a common good; taken to extremes, it can cause individual and sometimes community-wide harm. In the courtyard of our lives, curiosity can almost always be balanced with a healthy dose of “avert your eyes.”

“Need to know” is the information that people depend on to navigate modern society. Those who wish to make a living in the stock market “need to know” financial information. Weather forecasts help people and communities plan in large and small ways. Political information, construed broadly, is the lifeblood of democratic politics. Many have argued that the lack of political information is what allows dictators and oligarchs to flourish. For the courtyard to remain vibrant, people need to know what’s going on in the common space. To paraphrase Shakespeare, is the common garden weeded, or have the sewers backed up? The community as well as the individual is served. This is the compelling and philosophically-based rationale.

“Right to know” is information that is legally guaranteed—either in a positive way (an individual should have this information) or in a negative one (individuals have no right to this information because it places the community itself or its institutions at great risk). The revelations by Edward Snowden frame the complicated nature of the “right to know” debate in a century where political, economic, and governmental power appear to constitute some sort of political and economic conspiracy that is at once anti-democratic yet susceptible to forces such as non-state terrorism that threaten democratic communities across the globe. Philosophically, they ask us to consider whether it is only an “individual” who can see into the common courtyard, or whether...
governments (at best a community of individuals) or search algorithms (written by individuals but operating without human supervision) must be told to “seal the windows” shut.

Both the “right to know” and the “need to know” what is going on in the courtyard require sophisticated, analytic thinking and an awareness that not everyone—either people or institutions—is going to agree. Even tentative agreements, for example those called into question by Snowden’s revelations about the private facts of U.S. government surveillance in the service of the “war on terror,” ask people to rebalance their thinking about the relationship between individual and civil well-being. Whether you believe Edward Snowden is a “traitor” (the words of politicians as widely separated politically as President Barak Obama or radio talk show host Rush Limbaugh) or a “hero” (the view of many civil libertarians) may depend at the core on how you think about privacy and what weight you give its legal and philosophical roots.

Finally, there is the question of whether the unwanted gaze can simply forget what it saw. In an earlier time, one could wait for the story to die down, being available only to those who had access to a newspaper’s “morgue” or a television station’s extensive tape library. But few ordinary citizens could access these places, so a story would naturally die out. Today, however, with the Internet, anyone can access any stored information with just rudimentary knowledge of how to use a browser.

Most recently, law has been looked to as a remedy for this relatively new phenomenon of intrusive stories with an infinite lifetime—a decidedly twenty-first century notion of the right to be forgotten. In some parts of the world, the right to be forgotten is now considered a fundamental human right.

The history of the right began in 1998 when a Spanish newspaper published two announcements in its printed edition regarding the forced sale of properties arising from debts by the owner. A version was later made available on the newspaper’s website. In November 2009, the property owner requested the information about the sale be taken down for the newspaper’s website; the newspaper responded that because the report was a legal announcement, it would remain in perpetuity. The property owner then contacted Google about links to the site and then lodged a complaint with the Spanish Data Protection Agency, which ruled against Google—in essence telling the data conglomerate to remove links to the story—but upheld the right of the newspaper to retain the information on its website.

Out of the overlapping legal cases—which it is important to note had become global and involving multiple legal systems—the “right to be forgotten” emerged. That right had a cost: Spain no longer has “Google news.” The “right to be forgotten” mirrors the development of the larger “right to privacy” in that both are in the common law, often called the “discovered law” or law that emerges from lived experience. The concept of hezzek re’iyah does not kick in until urban living is the norm. The need for the “right to be forgotten” doesn’t occur until a medium, like the Internet, stores content in an easily-retrievable manner permanently.

The Technological Courtyard

Snowden and WikiLeaks also show that it is not just individuals who have private information. Revealing the private facts of corporate governance or statecraft also denotes a change in how people think about the courtyard that is at the philosophical root of Jewish law. The Talmud did not anticipate that the courtyard would become both global and virtual in the twenty-first century. Retaining control over content and context has never been easy, but the computer and its communication offspring have made reasoning through the philosophical thicket far more difficult.

Some suggest that in modern society the very notion of individual privacy is impossible. “Privacy is dead” headlines have been appearing since the 1990s (Sprenger, 1999). Donald Kerr,
deputy director of the U.S. Office of National Intelligence, told Newsday in 2007: “In our interconnected and wireless world, anonymity—or the appearance of anonymity—is quickly becoming a thing of the past.” In this view, technology simply makes it unrealistic to expect any serious protection from intrusion by government and corporations alike.

This is “big data,” a buzz word for the layers upon layers of information about individuals collected by a variety of institutions, connected to one another in ever more sophisticated ways, and then employed by everyone from pharmaceutical companies to web-based entities to both legacy and new media. While modern science is not quite there yet, many scholars believe that ultimately “big data” will include genetic information, a knowledge of “the self” on a cellular level which the philosophers who have written about privacy in past centuries almost certainly did not envision.

“Big data,” and even the not-so-big data that is currently the basis of commercially focused algorithms, raise ethical issues that have not been closely associated with the central ideas of individual “control” over information and “context” which dominated philosophical discussions about privacy. For example, technological intrusion suggests wealth could make privacy easier to maintain. “One key concern is that, as free Internet services become increasingly available, poorer consumers will sacrifice their privacy to receive free Internet access, whereas wealthier consumers will pay for Internet access and realize better privacy protection” (O’Neil, 2001, p. 29).

Wealth, however, is no guarantee. When fantasy sports teams became popular in the early years of this century, professional athletes, among the best paid celebrities, sued for invasion of privacy because their images and their athletic records had been appropriated without their permission for use in “fantasy leagues,” a form of on-line gambling popular in the developed West. Some have even predicted that as privacy continues to erode, users will be able to purchase their own privacy (Rust et al., 2002, p. 445) or at least privacy protection through commercial applications to guard against identity theft where those with the financial ability can be more secure in their information than those who cannot afford the service. Thinking about privacy in terms of wealth, as opposed to sophisticated analysis of context and control or through the lens of moral development (Kohlberg, 1981, 1984), invites discussion of distributive justice into the privacy conversation.

Another major concern expressed in the literature is that most people simply are not aware of the storage and use of their personal data online (Raab and Mason, 2004). In essence, they are unaware of the existence of the courtyard, the size of the common space, the sort of “neighbors” with whom they share the courtyard, or the various purposes, including economic ones, that sharing might support. As a result, Internet users focus on the benefits of their online transactions and believe they can take necessary precautions to minimize any anticipated risks despite multiple data hacks of institutions as disconnected as big-box retailers to the Internal Revenue Service (van de Garde-Perik et al., 2008). Internet users seem to view disclosure differently in social contexts such as blogs (Lee et al., 2008) and social networking sites.

In the past decade, Facebook has faced multiple protests over its changing privacy policies. And because technology is sometimes nimble, those who don’t like “Facebooking” their photos can simply transmit them over Instagram because, on that platform, users believe they do not become part of some “forever” data base. Both are profitable, global, and incompletely regulated by political communities.

However, the chances of a technological fix to the privacy problem, at least if the technology is a computer, reminds users that “anything can be hacked.” Many forms of technology seem to default to openness rather than privacy and require some knowledge and action on the part of the user to enhance privacy and security. In this century, technology is also firmly linked to the market.
The following themes emerge from these developments:

First, people do not consider privacy a monolithic category or good. They appear willing to negotiate its use under some conditions. This bolsters the conceptualization of privacy as an *a priori* right—a right that can be overwhelmed by other concerns. However, historically, those other concerns have focused on the needs of the political and social community; in the current context, market considerations plus other individual needs may also appear to justify openness where discretion may have been the norm in previous eras.

Second, the lack of transparency embedded in the technology itself may be a problem. The health of the community, particularly as defined by the philosophical notion of “flourishing” and the more discrete concept of economic well being, suggests that flourishing must take into account the equitable distribution of the privacy throughout the community. Google is a multi-national corporation and algorithms are “non-human,” but both are opaque as opposed to transparent in the distribution of “privacy.”

Further, the human decisions that form the basis of the corporate or machine-based choices are seldom well understood by the “end user.” The individuals making (or programming) them may fail to articulate the context and the “rules” of those choices to themselves or to others. Many such decisions are made by “entities” that reflect at least one degree of separation from a human being: computer programs called algorithms, a small procedure that mathematicians and computer scientists employ to solve a recurrent problem.

The word algorithm itself derives from the name of the mathematician, Mohammed ibn-Musa al-Khwarizmi, who was part of the royal court in Baghdad and who lived from about 780 to 850. When on-line commercial firms, everything from Amazon to eHarmony, make predictions about what customers would like from books, to gadgets, to possible partners, they do so based on algorithms—computer programs which, at their apex, have some capacity to “learn” or teach themselves more sophisticated approaches to solving specific problems, for example, playing chess. Algorithms currently are employed in three very broad ways: for commercial applications, by governments for security purposes, and by mathematicians and computer scientists engaged in research. Commercial applications and governments attempting to ensure security in this century challenge the individual’s ability to assert privacy claims over information. They also sometimes subvert existing community-based political and legal understandings. When confronted with a large corporation or government entity, individual choice may well be an inadequate mechanism to reassert control over both information and the context in which it is understood. Historically, people have turned to the law to balance the power equation in such circumstances.

However, the law is almost always post hoc, one of the often stated concerns about the harm that loss of privacy entails (Alderman and Kennedy, 1995). Privacy, once lost, is almost impossible to recover. So, when individual privacy is the focus of concern, institutions may well have affirmative obligations to safeguard privacy—essentially acting in such a way as to forestall privacy invasion in much the same way that corporations and governments have an obligation to ensure consumer and citizen safety in certain conditions. While these obligations are enforced through the law, the law here has its roots in philosophy, specifically the affirmative duty to prevent harm or do as little harm as possible as articulated in the work of philosophers such as John Stuart Mill and W. D. Ross. Thus, third parties such as dating websites or health care systems can be reasonably assumed to have an ethical obligation not only to safeguard data but also to craft thinking about privacy into the increasingly sophisticated algorithms and other forms of artificial intelligence that currently constitute the collection and use of information for the varied purposes to which data can be put.

Cumulatively, these twenty-first century understandings about the needs for and components of the philosophical “good life” argue for the development of an institution-based ethics of privacy.
A Conceptual Bridge: Contested Commodities

As the foregoing indicates, privacy is most often taught and understood as either the province of law or the province of philosophy. Technology is incompletely connected to both. Scholars appear to pick a “domain” and stick to it.

Legal scholar Margaret Radin (1982, 1993, 1996) is one of few who has taken understandings from law and philosophy to develop new theory. Radin has developed the concept of contested commodities to explain how the concept of personhood, as articulated by philosophers David Hume, Thomas Hobbes, Kant, J. S. Mill and feminist philosophy, can critique and inform traditional market economics where the concept of personhood and private property which can be bought and sold are inextricably joined.

Radin begins with a theory of the self that owes some of its conceptual power to feminist ethics, particularly those outlined by Nussbaum (2003; 2011) and the capabilities approach.

When the self is understood expansively so as to include not merely undifferentiated Kantian moral agency but also the person’s particular endowments and attributes, and not merely those particular endowments and attributes, either, but also the specific things needed for the contextual aspect of personhood, then this understanding is a thick theory of the self. A thick theory of the self correlates with an expansive role for inalienability because things that are understood as inside the self, or as bridging the boundary between inside and outside, cannot simultaneously be understood as readily detachable from the self they constitute.

Radin embodies the community in the self but also situates the self within community, a defining feature of the capabilities approach because it also takes social institutions and people’s capabilities to act within them and because of them into account.

Radin’s “thick theory of the self” builds on the work of Naussbaum to explore the functions of private property in a capitalistic market, noting that market language does not always best describe certain human activity. Consider a wedding ring, which is purchased for a specific “price” at the beginning of many relationships. Add 36 years of marriage, a trio of kids, some illness, and some joy, and the “price” of the wedding ring no longer represents the “value” of the marriage. Indeed, that value is probably best expressed, not in the language of the market, but in the language of the poet or of the philosopher or of the psychologist.

Money is no longer the object of affection. And, this is despite the fact that marriage has both economic benefits and costs.

Radin asserts that a thick theory of the self and the traditional concepts of market-driven economics do co-exist within contemporary culture, but that there is a group of “goods”—contested commodities like the wedding ring example—for which market economics does not provides complete explanatory power. It is within the language of her work to assert that private information which emerges from human beings acting within a cultural context constitutes a contested commodity, one which market forces may intrude upon but which are incompletely accounted for by examining only market transactions. Radin’s theory is rooted in Naussbaum’s concept of human capabilities, included among them free expression, association, control over one’s environment, and the human capacity for imagination and thought. Human capabilities constitute the contemporary core of what the Greeks described as flourishing.

Privacy as a contested commodity fits well with twenty-first century lived experience at the individual level—that privacy is an a priori right that individuals can chose to trade away, or to retain, based on individual needs and desires. The concept of contested commodity also notes that the “contest” takes place not just within an isolated individual but within an individual who
is also embedded in a cultural and economic system. Finally, that “contest” is in the service of human capabilities—capabilities which can be actualized in a community and within certain sorts of markets, but are also separable from them in individual circumstances, for example the wedding ring illustration noted above. Because it takes place within a social and cultural system, an essential component of Nussbaum’s normative conceptualization of the human capabilities, the theory of contested commodity may also apply when technology enters the arena.

BUILDING AN INSTITUTION-BASED THEORY OF PRIVACY

Based on the lives we live in this century and on the philosophical concept of human capabilities as articulated by Nussbaum, any theory of privacy at the institutional level must combine elements of ethics, law and a dynamic understanding of technology. The institutional-level of analysis assumes that individuals, the focus of most philosophical theory about privacy, maintain a necessary symbiotic relationship with social and cultural institutions without which fulfilling some capabilities such as association and control over one’s environment would be impossible. This institutional-level approach also eschews one of the major tenants of contemporary philosophy: that institutions are not “people” and cannot be treated philosophically as entities with the capacity to form intent, to make moral choice, or to be held morally accountable (May, 1987).

A contemporary institutional theory of privacy takes its understanding of the need for ethical responsibility from the law which has codified the understanding that institutions can be held accountable for acts which are essentially ethical in nature (Noddings, 1989). It also accepts contemporary research on organizations that documents organizational “cultures” which can promote as well as retard ethical actions by employees at all levels of responsibility and authority (Barnett and Vaicys, 2000). Finally, it accepts a more ancient understanding of politics, dating at least to Plato and Aristotle but continuing through many articulations of democratic theory: some forms of government make it more possible to behave ethically than do others. To summarize, an institution theory of privacy asserts that institutions matter to both how people conceptualize privacy in their individual lives (Vallor, 2016) and to how they can achieve it within community. Just as the individual works with conceptualizations of right to know, need to know and want to know, an institutional-based theory of privacy should consider the following circles of responsibility.

Outermost Level of Responsibility: Responsibility to the Consumer

In the role of individual-as-consumer, privacy would be a contested commodity. The capacity for and distribution of individual harm and good which corporate-based privacy decisions could promulgate would require transparent and future-oriented evaluation at the community level. Here, even though temptation is great, market forces alone would provide a less compelling privacy argument than philosophical and political concepts of flourishing—a rough parallel between the distinctions of want to know and need to know, where market forces are not trivial but must be considered within a web of more compelling and human-centered arguments. Institutions within society would be charged with overseeing, through self-regulation and government regulation, the equitable distribution of the “good” of privacy to various social groups; within this emerging law, corporations could be held accountable for the economic consequences of privacy invasion. A contemporary example of this approach is the recent court decision involving Gawker Media, where various court rulings have amounted to an acknowledgement that privacy may be considered an individual economic asset (Bollea v. Gawker Media).
Second Level of Responsibility: Intersection of Citizen and State

The more disconnected the ability to make ethical decisions is from an individual moral intelligence, the more carefully circumscribed and routinely evaluated artificial intelligence and the uses to which it is put in information collection must be evaluated by the political community. So must institutional-based programs and regulations. This preliminary maxim would also be the subject of evaluation through lived experience; people might agree that various forms of artificial intelligence could help to design biologically specific anti-cancer treatments but reject a similar use for evaluating internet searches in the hopes of discovering future terrorist activity.

Here, the institutions involved would have an affirmative responsibility to demonstrate that such activity would not have a negative impact on human capabilities as outlined by Nussbaum. Although this sounds contradictory, it is in no way different than the regulations governing drug development; pharmaceutical corporations have to demonstrate that what they propose will cause harm to human beings only within certain limits. It is acknowledged that the intersection of the citizen and the state over private information will change as time and technology change. Privacy as a contested commodity would default to openness at the institutional level; institutions would be expected to be transparent about what they do and how their actions impinge on individual privacy. However, at the individual level, discretion would be the default. People would have to decide to opt-in to certain sorts of arrangements, particularly those that can have negative consequences on their health or psychological well being or on their ability to function within a vibrant community. It is acknowledged that there may be substantial and sometimes unintended overlap between the institutions of the market and of politics.

For Journalists: Responsibility for Reporting the Philosophical and Economic Claims about Privacy as News

Here it is the flourishing of the community that takes precedence, but that flourishing must also include an analysis of individual actualization of capabilities over time and the just distribution of the “right” to privacy community wide. Such a conceptualization of privacy requires an articulated balancing of minority and majority capabilities and rights—an acknowledgement that both philosophy and law have a role to play in evaluating how institutions influence individual lives when the issue is privacy.

Technology here is a servant, but is also acknowledged to have moral weight in privacy decisions. Thus, the journalistic role begins with reporting and writing the news in such a way as to minimize the harm of privacy invasion, including emerging news technologies such as the 360-degree camera or the use of drones and virtual reality to report news events. This is a daunting effort for journalists, but to it they must add the beat of “privacy” as it is reflected in economic decisions and through legislation. This effort will require assertive reporting on issues that both journalists and the public are only just now beginning to understand and one in which news organizations themselves are important actors. Privacy, when it becomes news, is more about “why” and “how.” The best stories will focus on the places where law, philosophy and technology intersect. To some extent, this convergence of insights over one extraordinarily important issue has been anticipated. In Patterson v. Tribune, the Tampa Tribune disclosed the commitment of a woman to a narcotics-recovery facility, an act prohibited by Florida statute. In finding for the plaintiff, the court noted: “Our metropolitan newspapers … are the technological marvels of our age. They render invaluable public service … almost political in their capacity to influence public opinion, rightly blest with the constitutional guaranty of freedom of the press. Such power imposes corresponding responsibility.” When the issue is privacy, the responsibility
is shared, not just by individuals but by the community that forms around the common courtyard of human life. Privacy theory crosses boundaries. It enlarges the concept of flourishing—and any potential harms to that process—beyond the individual to the community and culture that allows people to realize their greatest happiness.

The recent debate over the programming protocol for the eminent driverless car serves as an example of an institution—the transportation industry—making an essentially moral choice and being held morally accountable (Greene, 2016). Though accidents caused by the driverless car will be virtually non-existent, programmers universally agree, accidents will happen largely because of human error by others on the road—motorists, bicyclists and pedestrians—that will essentially force the driverless car to make a “choice” to save the life of its occupant or possibly save others on the road including those who might have been at fault in the first place. Solving this real life trolley problem will require utilitarian thinking: doing the least amount of harm for the most people.

This illustration sums up the privacy conundrum and the need to acknowledge that law, philosophy and technology will intersect in novel ways to respond to it. The decision to open oneself to the world’s courtyard voluntarily is a “risk”—that private thoughts might be flung to the outer circle of intimates—in exchange for the “reward” of full participation in a modern democratic society which cannot function as a community without this sort of participation. Individuals may take such risks for economic reasons, but those risks need to be taken in an institutional context that regards privacy as both a right and a “need” that allows humans to fulfill their capabilities. Law that restricts institutions thus becomes the “tracks” that the trolley travels on. But, how that trolley car is engineered—to safeguard those who ride it—will be the province for both law and ethics. The power of big data, meta-data and algorithms must include the concept of human-based discretion—an ethical equation—if privacy is to be preserved. In the modern era, preventing 1984 or the Republic of Panem will require the injection of ethical thinking at every level of human-based or human-originated activity, including a reframing of how philosophers consider the moral weight of institutional choice.

REFERENCES


