Privacy, Neuroscience, and Neuro-Surveillance

Adam D. Moore

Res Publica
A Journal of Moral, Legal and Social Philosophy

ISSN 1356-4765

Res Publica
DOI 10.1007/s11158-016-9341-2

Springer

Res Publica
DOI 10.1007/s11158-016-9341-2

Privacy, Neuroscience, and Neuro-Surveillance

Adam D. Moore[1]

Abstract The beliefs, feelings, and thoughts that make up our streams of consciousness would seem to be inherently private. Nevertheless, modern neuroscience is offering to open up the sanctity of this domain to outside viewing. A common retort often voiced to this worry is something like, 'Privacy is difficult to define and has no inherent moral value. What's so great about privacy?' In this article I will argue against these sentiments. A definition of privacy is offered along with an account of why privacy is morally valuable. In the remaining sections, several privacy protecting principles are defended that would limit various sorts of neuro-surveillance promised by advancements in neuroscience.

Keywords Privacy · Privacy rights · Neuroscience · Neuro-surveillance · Brain-privacy · Notice · Consent · Probable cause · Waiving privacy · Privacy as property

Our beliefs, feelings, and the ticker-tape of words, images, and thoughts that make up our streams of consciousness would seem to be inherently private. Nevertheless, modern neuroscience is offering to open up the sanctity of this domain to outside viewing. We may be able to find out what other people think, covertly and without permission. It may be possible to 'extract private information about users' memories, prejudices, religious and political beliefs, as well as about their possible neurophysiological disorders' (Bonaci et al. 2014, p. 1). Bonaci et al. even highlight the first example of brain 'spyware'. In this case, recorded electroencephalography (EEG) information was used to extract private information 'such as credit card PIN's, dates of birth and locations of residence' (2014, p. 1; Martinovic et al. 2012).

✉ Adam D. Moore
moore2@u.washington.edu

[1] University of Washington, Information School, Box 352840, Mary Gates Hall, Ste 370, Seattle, WA 98195-2840, USA

Published online: 04 November 2016

Neuromarketing promises to allow companies to better pitch products and services based on information scanned from reward-related areas of the brain (Haynes 2012).

A quick survey of recent articles related to privacy and neuroimaging include titles such as 'Scientists Can't Read Your Mind with Brain Scans Yet', 'Neuroscience: The Mind Reader', and 'Brain Says Guilty! Neural Imaging may Nab Criminals' (Miller 2014; Cyranoski 2012; Lewis 2013). These alarmist titles indicate more of a direction than a description of the current state of brain scanning. Nevertheless, one might wonder to what extent current brain-imaging technology impacts individual privacy rights to thoughts, feelings, dispositions, or biases.

The technology being used, advanced, and refined is dizzyingly wide ranging and complex. From EEG and magnetoencephalography (MEG) to magnetic resonance imaging (MRI) and functional magnetic resonance imaging (fMRI), along with numerous other neuroimaging techniques, there seems to be an ever-growing list of ways to potentially peer into the thoughts of human beings (Hallinan et al. 2014, p. 58). Beyond neuroimaging, brain-computer interfaces (BCIs) are being developed for both medical and non-medical purposes (Bonaci et al. 2014). Moreover, consider predictive analytics focused on human behavior. Machine learning and big-data analysis, along with complex predictive modeling, may be able to determine what someone is thinking simply by looking at human behavior.

While currently limited, modern neuroscience and other technologies are promising access to the sanctuary of our private thoughts (Hart et al. 2000; Farah et al. 2008; Gligorov and Krieger 2010; Fischbach and Mindes 2011; Richmond et al. 2012; Chekroud et al. 2014; Bonaci et al. 2014). But this is something we have always confronted. From Gutenberg's press to photography, videos, and genome mapping, we seem to be constantly pushing further into the private lives of individuals. Justice Douglas, dissenting in the famous privacy case *Osborn v. United States* (1966) noted:

> The time may come when no one can be sure whether his words are being recorded for use at some future time; when everyone will fear that his most secret thoughts are no longer his own … when the most confidential and intimate conversations are always open to eager, prying ears. When that time comes, privacy, and with it liberty, will be gone. (385).

Socrates once said that 'the unexamined life is not worth living'—but he was talking about self-examination, not the public examination of private areas, thoughts, or beliefs.

One common retort that I often hear is something like, 'What's so great about privacy?' Scholars lament that privacy is a fuzzy concept—there is no agreed-upon definition. Others claim that, aside from being difficult to define, privacy is culturally relative and has no inherent moral value (see Lever 2012). I have argued against these sentiments (Moore 2003, 2008, 2010). A coherent, defensible definition of privacy can be offered. Moreover, I have defended a particular conception of privacy against rival views by showing its connection to human wellbeing or flourishing. In the first part of this article, I will attempt to capture the essence of my preferred view of privacy and why it should be rationally endorsed.

In the remaining sections, I will address what, if anything, should be done about the tensions between privacy and modern neuroscience.

Establishing a Moral Presumption in Favor of Privacy[1]

There are two distinctions that have been widely discussed related to defining privacy. The first is the distinction between descriptive and normative conceptions of privacy. A descriptive or non-normative account describes a state or condition where privacy obtains. An example would be Parent's definition, '[p]rivacy is the *condition* of not having undocumented personal knowledge about one possessed by others' (Parent 1983, p. 269). A normative account, on the other hand, makes references to moral obligations or claims. For example when DeCew talks about what is of 'legitimate concern of others' she includes ethical considerations (DeCew 1997, p. 60).

One way to clarify this distinction is to think of a case where the term 'privacy' is used in a non-normative way such as someone saying, 'When I was getting dressed at the doctor's office the other day I had some measure of privacy.' Here it seems that the meaning is non-normative—the person is reporting that a condition obtained. Had someone breached this zone the person may have said 'You should not be here, please respect my privacy!' In this latter case, normative aspects are stressed.

Reductionist and non-reductionist accounts of privacy have also been offered. Reductionists, such as Judith Jarvis Thomson, argue that privacy is derived from other rights such as life, liberty, and property rights—there is no overarching concept of privacy but rather several distinct core notions that have been lumped together (Thomson 1975). Viewing privacy in this fashion might mean jettisoning the idea altogether and focusing on more fundamental concepts. For example, Frederick Davis has argued that, '[i]f truly fundamental interests are accorded the protection they deserve, no need to champion a right to privacy arises. Invasion of privacy is, in reality, a complex of more fundamental wrongs. Similarly, the individual's interest in privacy itself, however real, is derivative and a state better vouchsafed by protecting more immediate rights' (Davis 1959, p. 20). Unlike Davis, the non-reductionist views privacy as related to, but distinct from, other rights or moral concepts.

It is my view that the normative and non-normative distinction is important and crucial for conceptual coherence—it is possible and proper to define privacy along normative and descriptive dimensions. Liberty is also defined descriptively and normatively. We may, for example, define liberty without making any essential references to normative claims. Thomas Hobbes defines liberty as 'the absence of external impediment' (Hobbes 1985, p. 189). In this example, as with Hobbes's conception of the state of nature, there no moral 'oughts' or 'shoulds' present.

[1] Parts of this section draw from material originally published in Moore, A., *Privacy rights: Moral and legal foundations,* Chaps 2–3 (2010); 'Defining privacy' (2008); and 'Privacy: Its meaning and value' (2003).

Alternatively, J. S. Mill defends a normatively loaded account of liberty opening his classic work *On Liberty* with 'The subject of this essay is… civil, or social liberty: the nature and limits of the power which can be legitimately exercised by society over the individual' (Mill 1859, p. 1). Privacy may also be defined descriptively or normatively.

Second, assuming a normative definition, without considering the justification of the rights involved it is unclear if privacy is reducible to other rights or the other way around. This point has been made by Parent and others (Parent 1983; DeCew 1997). Moreover, given the arguments that I offer elsewhere, it is not surprising that there are close connections between privacy, liberty, and self-ownership rights (Moore 2001, 2007). It is also true that the kind of rights involved will be intimately tied to the form of justification—it would be surprising to find hard-line Kantians and crude consequentialists arriving at the same conception of 'rights'. And even if the reductionist is correct it does not follow that we should do away with the category of privacy rights. The cluster of rights that comprise privacy may find their roots in property or liberty yet still mark out a distinct kind. Finally, if all rights are nothing more than complex sets of obligations, powers, duties, and immunities it would not automatically follow that we should dispense with talk of rights and frame our moral discourse in these more basic terms.

While privacy has been defined in many ways over the last century, I favor what has been called a 'control'-based definition of privacy (see Warren and Brandeis 1890; Westin 1967; Gross 1971; Parker 1974; Parent 1983; Allen 2003; Gavison 1983). A right to privacy is a right to control access to, and uses of, places, bodies, and personal information (Moore 2003, 2008, 2010). For example, suppose that Smith wears a glove because he is ashamed of a scar on his hand. If you were to snatch the glove away, you would not only be violating Smith's right to property, since the glove is his to control, but also his right to privacy—a right to restrict access to information about the scar on his hand. Similarly, if you were to focus your x-ray camera on Smith's hand, take a picture of the scar through the glove, and then publish the photograph widely, you would violate a right to privacy. While your X-ray camera might diminish Smith's ability to control the information in question, it does not undermine his right to control access (Moore 2007).

Privacy also includes rights concerning the use of bodies, locations, and personal information. If access is granted accidentally or otherwise, it does not follow that any subsequent use, manipulation, or sale of the good in question is justified. In this way, privacy is both a shield that affords control over access or inaccessibility, and a kind of use- and control-based right that yields justified authority over specific items, such as a room or personal information (Moore 2007). For example, by appearing in public and leaving biological matter behind, someone might grant access to specific sorts of personal information. We should not conclude, however, that by granting a particular kind of access, the individual has also waived control over any and all future uses of the biological matter or the information found within.

A serviceable definition of 'personal information' is provided by the European Union Data Directive. Personal information is 'any information relating to an identified or identifiable natural person … one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more

factors specific to his physical, physiological, mental, economic, cultural or social identity' (Directive 95/46/EC of the European Parliament and of the Council [1995] OJ L 281 0031–0050). For example, information about a specific individual's sexual orientation, medical condition, height, weight, income, home address, phone number, occupation, and voting history would be considered personal information on this account.

Judith Jarvis Thomson finds control-based definitions of privacy puzzling. She argues that a loss of control does not always mean that we have lost privacy:

> If my neighbor invents an X-ray device which enables him to look through walls, then I should imagine I thereby lose control over who can look at me: going home and closing the doors no longer suffices to prevent others from doing so. But my right to privacy is not violated until my neighbor actually does train the device on the wall of my house (Thomson 1975, p. 304. n. 1).

First, it is important to note how Thomson slides between non-normative and normative control-based accounts of privacy in this case. At the start of the case control is lost but privacy is maintained because the individual who now has control does not exercise it. A control-based *condition* of privacy no longer obtains, yet a privacy right has not been violated. Sure enough this sounds odd—but it is odd because I do not think that control-based privacy theorists actually intend to support a purely non-normative conception of privacy. To put the point another way, if we sprinkle normativity, so to speak, throughout the definition—privacy is an access control and use right to places, bodies, or personal information—then Thomson's attack loses its force. Simply put, a condition of privacy obtains when others do not have access while a right to privacy affords control over access and use independently of whether condition of privacy holds.

Thomson continues with a second example. 'Suppose a more efficient bugging device is invented: instead of tapes, it produces neatly typed transcripts (thereby eliminating the middlemen). One who reads those transcripts does not hear you, but your right to privacy is violated just as if he does' (Thomson 1975, p. 304, n. 1). But this case fits well with the view of privacy rights as justified control over access to objects and information. Information may take many forms and thus it may be accessed in many different ways. If an individual has a right to control access to and uses of some bit of information, then it does not matter *how* the information was accessed—what matters is *that* it was accessed. Thomson claims while '[y]ou may violate a man's right to privacy by looking at him or listening to him; there is no such thing as violating a man's right to privacy by simply knowing something about him' (Thomson 1975, p. 307). This seems true enough. However, by *looking* or *listening* you may be violating his right to control access to information—information that provides the foundation for 'knowing'. Moreover and more importantly, you may be violating a use control right. If correct, it would seem that Thomson's critique of control-based definitions of privacy fails.

Turning now to questions of value, there is evidence that the ability to control access to places, bodies, and personal information is important for human wellbeing. Note that if I am correct about the objective, yet culturally dependent, value of privacy, then something universal will have been established. Privacy is valuable for

the same reasons whether one is a citizen of the USA, the EU, or a member of an indigenous group. Moreover, unless value-based consequences play no role in determining our moral and political obligations, the importance of including privacy-based considerations will have been highlighted.

To get a sense of why privacy is essential for human wellbeing it is helpful to consider interests in separation that are shared by many non-human animals. While privacy rights may entail obligations and claims against others—obligations and claims that are beyond the capacities of most non-human animals—a case can still be offered in support of the claim that separation is valuable for animals. In *Privacy and Freedom*, Alan Westin (1967) notes:

> One basic finding of animal studies is that virtually all animals seek periods of individual seclusion or small-group intimacy. This is usually described as the tendency toward territoriality, in which an organism lays private claim to an area of land, water, or air and defends it against intrusion by members of its own species. (p. 8)

More important for our purposes are the ecological studies demonstrating that a lack of private space, due to overpopulation and the like, will threaten survival. In such conditions, animals may kill each other or engage in suicidal reductions of the population. Given the similarities between humans and many non-human animals, it is plausible to think that we share many of the same traits. For example, Lewis Mumford notes similarities between rat overcrowding and human overcrowding: 'No small part of this ugly urban barbarization has been due to sheer physical congestion: a diagnosis now partly confirmed by scientific experiments with rats—for when they are placed in equally congested quarters, they exhibit the same symptoms of stress, alienation, hostility, sexual perversion, parental incompetence, and rabid violence that we now find in large cities' (Mumford 1961, p. 210). These results are supported by numerous studies conducted more recently. Household overcrowding and overcrowding in prisons have been linked to violence, depression, suicide, psychological disorders, and recidivism (see Baum and Koman 1976; Clauson-Kaas et al. 1996; Edwards and Booth 1977; Fuller et al. 1996; Morgan 1972; Farrington and Nuttall 1980; Paulus et al. 1978; Cox et al. 1984; McCain et al. 1980; Ruback and Carr 1984; Megargee 1977; Porporino and Dudley 1984).

Cultural universals have been found in every society that has been systematically studied (see Murdock 1955; Nussbaum 2000). Based on the Human Relations Area Files at Yale University, Alan Westin has argued that there are aspects of privacy found in every society—privacy *is* a cultural universal (Westin 1967; Roberts and Gregor 1971). While privacy may be a cultural universal necessary for the proper functioning of human beings, its form—the actual rules of association and disengagement—is culturally dependent (see Spiro 1971). The kinds of privacy rules found in different cultures will be dependent on a host of variables including climate, religion, technological advancement, and political arrangements. Nevertheless, I think it is important to note that relativism about the forms of privacy—the rules of coming together and leave-taking—does not undermine my claim regarding the objective need for these rules. There is strong evidence that the ability to

regulate access to our bodies, capacities, and powers and to sensitive personal information is an essential part of human flourishing or wellbeing.

In an important article dealing with the social psychology of privacy, Barry Schwartz (1968) provides interesting clues as to why privacy is universal (also see Mill 1859; Rachels 1975). According to Schwartz, privacy is group preserving, maintains status divisions, allows for deviation, and sustains social establishments (1968, p. 741). Privacy also preserves groups by providing rules of engagement and disassociation. Without privacy, or what may be called a dissociation ritual, there could be no stable social relations. As social animals, we seek the company of our fellows, but at some point, interaction becomes bothersome and there is a mutual agreement to separate. Thus, having 'good fences' would be necessary for having 'good neighbors' (Rachels 1975, p. 331).

Schwartz also notes that privacy helps to maintain status divisions within groups. A mark of status is a heightened level of access control. Enlisted men in the armed services have less privacy when compared to commissioned officers. Line-level employees work without doors or secretaries. By protecting status divisions and determining association and disassociation rules, privacy has a stabilizing effect on groups or social orders (see McGinley 1959, p. 56). Privacy also protects and leaves room for deviation within groups. As J. S. Mill noted in *On Liberty* (1859, Chap. 2) when individuals engage in different forms of living, protected by the walls of privacy, new ideas are produced and, if good, are adopted.

Growing up can be understood as the building of a series of walls—the walls of privacy. 'Both animals and humans require, at critical stages of life, specific amounts of space in order to act out the dialogues that lead to the consummation of most of the important acts of life' (Spitz 1964, p. 752). Infants are without privacy. As infants grow into toddlers and begin to communicate with language, they express wishes for separation at times. This process continues as children grow into adults. 'The door of openness closes perhaps halfway as a recognition of self-development during childhood, it shuts but is left ajar at pre-puberty, and closes entirely—and perhaps even locks—at the pubertal and adolescent stages when meditation, grooming, and body examination become imperative' (Schwartz 1968, p. 749; also see Erikson 1963; Kessler 1966). Toddlers and small children begin requesting privacy as they start the process of self-initiated development. More robust patterns of disassociation continue as children enter puberty. Finally, as young adults emerge, the walls of privacy harden, and access points are maintained vigorously.

A recent article presents additional compelling evidence that privacy is essential for flourishing and wellbeing (Newell et al. 2015). Children who are monitored by parental solicitation or with the use of rule sets (you have to be home by 7 p.m., no playing with this or that kid, etc.) have the same rate of problematic behavior as kids who are not monitored at all. '[C]ross-sectional and longitudinal studies show that poorly monitored adolescents tend to be antisocial, delinquent, or criminal … [they] also tend to use illegal substances … tobacco … do worse in school … and engage in more risky sexual activity' (Stattin and Kerr 2000b, p. 1072). However, where there is two-way communication between parents and children, when all are actively participating, including the voluntary sharing of information, there is an associated drop in the behaviors mentioned above. In a follow-up article, Kerr and

Stattin conclude, '[I]t appears that the less effective strategy, and the one that has the potential of backfiring, is to try to prevent adolescents from getting into trouble by rigorously controlling their activities and associations' (2000a, p. 378; also see Hare et al. 2011; Barnes et al. 1994; Kafka and London 1991; Eaton et al. 2009). There are obvious and strong connections between flourishing or well-being and privacy for adolescents. Furthermore, problematic behavior or 'poor adjustment', including depression, violent outbursts, and risky sexual behavior, increases with the loss of privacy and control (Kerr and Stattin 2000a, p. 366).

Having said something about what a right to privacy is and why it is valuable, we might ask how privacy rights are justified (Moore 2007, 2010). A promising line of argument combines notions of autonomy and respect for persons. A central and guiding principle of Western liberal democracies is that individuals, within certain limits, may set and pursue their own life goals and projects (Lever 2016). Rights to privacy erect a moral boundary that allows individuals the space to order their lives as they see fit. Clinton Rossiter puts the point succinctly:

> Privacy is a special kind of independence, which can be understood as an attempt to secure autonomy in at least a few personal and spiritual concerns, if necessary in defiance of all the pressures of the modern society … It seeks to erect an unbreachable wall of dignity and reserve against the entire world. The free man is the private man, the man who still keeps some of his thoughts and judgments entirely to himself, who feels no over-riding compulsion to share everything of value with others, not even those he loves and trusts. (1958, p. 17)

Privacy protects us from the prying eyes and ears of governments, corporations, and neighbors. Within the walls of privacy, we may experiment with new ways of living that may not be accepted by the majority. Privacy, autonomy, and sovereignty, it would seem, come bundled together.

A second but related line of argument rests on the claim that privacy rights stand as a bulwark against governmental oppression and totalitarian regimes. If individuals have rights to control personal information and to limit access to themselves within certain constraints, then the kinds of oppression that we have witnessed in the twentieth century would be nearly impossible. Put another way, if oppressive regimes are to consolidate and maintain power, then privacy rights, broadly defined, must be eliminated or severely restricted. If this is correct, privacy rights are a core value that limits the forces of oppression (Westin 1967; Schoeman 1992; DeCew 1997; Rössler 2005; Moore 2010; Allen 2011; Nissenbaum and Brunton 2015).

Arguably, any plausible account of human wellbeing or flourishing will have a strong right to privacy as a component. Controlling who has access to us is an essential part of being a happy and free person. This may be why 'peeping Toms' are held up as moral monsters—they cross a boundary that should never be crossed without consent.

Each of us has the right to control our own thoughts, hopes, feelings, and plans, as well as a right to restrict access to information about our lives, family, and friends. I would argue that what grounds these sentiments is a right to privacy—a

right to maintain a certain level of control over personal information. While complete control of all our personal information is a pipe dream for many of us, simply because the information is already out there and most likely cannot or will not be destroyed, this does not detract from the view of personal information ownership. Through our daily activities, we each create and leave digital footprints that others may follow and exploit—and that we do these things does not obviously sanction the gathering and subsequent disclosure of such information by others.

Whatever kind of information we are considering, there is a gathering point where individuals have control. For example, when we purchase a new car and fill out the loan application, no one would deny that we each have the right to demand that such information not be sold to other companies. I would argue that this is true for any disclosed personal information, whether it be patient questionnaire information, video-rental records, voting information, or credit applications. To agree with this view, one first has to agree that individuals have the right to control their personal information—i.e. binding agreements about controlling information presuppose that one of the parties has the right to control this information.

If all of this is correct, then we have a fairly compelling case in support of the view that individuals have moral claims to control access to and uses of specific places and things, as well as certain kinds of information—i.e. we have established a presumption in favor of privacy (Moore 2010; Westin 1967; DeCew 1997; Rössler 2005; Nissenbaum 2009; Allen 2011).

Privacy-Protecting Principles

As noted above, I think that privacy is morally valuable and individuals have privacy rights. Privacy, defined as a right to control access to and uses of places, bodies, and personal information, is morally valuable for human beings (Moore 2003, 2008, 2010). Simply put, violating the norms around leave-taking and control over access causes measurable objective harms. Nevertheless, even if this is true, privacy rights are not absolute. There may be times when such boundary crossings are justified. But note where the burden of justification rests. To override individual rights to privacy, the burden of proof rests on those who would cross into private domains. Consider how far away this guideline is from current practice. In almost every area of technological advancement, the question is not '*should* we monitor, track, hoard, aggregate, and search ever-increasing amounts of data', or 'will these advancements violate privacy rights?' The guiding principle seems to be a question of 'is', not 'ought'—of what *is* possible, not what we *should* do or allow. We can do these things, so it seems that, almost unthinkingly, we roll them out and worry about the 'ought' and 'value' issues later. Modern advances in neuro-surveillance appear to be no different. *Can* does not imply *should*. If we start with a presumption of privacy, however, these impulses will be muted. The privacy protecting principles outlined below are offered as guidelines so that we do not continue to make these sorts of mistakes.

Setting aside the current state of brain imaging or scanning, and the technologies that allow information to be extracted from our brains and cognitive processes,

imagine what might be the case in the coming decades (Moreno 2011; Farah 2011). Suppose we could view your brain at work and discover that you are prejudiced against women or homosexuals. Imagine if your employer could determine susceptibility to depression, violent impulses, or lack of empathy. Your boss might find such information useful, especially for the purposes of limiting company exposure to lawsuits, lost sales, or theft. Along with the standard personality tests, most businesses might require multiple brain scans under various conditions to further determine the 'type' of person you are.

We can imagine that neuromarketing has advanced so that advertisers know what you like, prefer, or despise independent of your stated beliefs or opinions. Tracking the pleasure centers of your brain, recording facial expressions, and comparing such data to baseline information may allow advertisers to more accurately pitch products and services. Brokers could sell or trade this information. Predictive analytics coupled with neuro-surveillance could provide more powerful tools.

Consider how such technology could be used in the courtroom. 'Brain fingerprinting' to detect lies is an area of current research (Finn 2006; Federspiel 2008; Murphy and Greely 2011; Haynes 2012; and Farahany 2012). Suppose that, along with subpoenaing baseline neurological scans from various third parties, law enforcement could also monitor a suspect's brain activity under questioning. In the United States, the Fifth Amendment's protection against 'self-incrimination' has been interpreted to apply to testimony, not physical evidence. The question at hand is whether third-party neurological scans or real-time monitoring of a suspect's brain while they are under questioning is testimony, physical evidence, or none of the above.

Numerous other examples of the advancing tensions between neuroscience and privacy could be presented. What follows, however, are several privacy-protecting principles offered as guidelines for adjudicating these tensions. Understandably, it is impossible to foresee all the ways privacy may be implicated with advancements in neuroscience. Likewise, it is impossible to know all the ways neuroscience might develop to enhance, rather than undermine, individual privacy rights. By offering these guidelines, my hope is to avoid making the sorts of ethical mistakes that we have made in the past.

Privacy as Property

While numerous authors have considered the strengths and weaknesses of viewing privacy as a kind of property (see Laudon 1996; Samuelson 2000; Lessig 2002), I think there are advantages to this approach. If the definition of privacy that I have offered is compelling, then the correct way to view privacy is as a kind of property claim. Furthermore, if this definition of privacy is connected to moral value, as I have argued, then we will have good reasons for viewing privacy in this way.

Instead of viewing privacy as a mere interest, a subjective expectation or preference, imagine if it were understood as a form of property. If property rights and privacy rights are both essentially about control, then maybe privacy rights are simply a special form of property rights. Intellectual property is generally characterized as non-physical property where owner's rights surround control of

physical manifestations or 'embodied ideas'. Intellectual property rights center on control of physical items, and this control protects rights to ideas; for example, no matter how a specific poem is instantiated (written, performed orally, or saved on a website) copyright would apply. Rights to control physical goods, on the other hand, allow control over one physical object.

Privacy may be understood as a right to control access to and uses of places and ideas independent of instantiation. Physical privacy yields rights to control access to one's body or specific places. Informational privacy, on the other hand, is more like a copyright. No matter how the information is codified, a rights-holder would have control over access to and uses of the information. Warren and Brandeis are correct to note that copyright protects expressions, not the ideas that make up the expressions, and thus privacy cannot be captured under copyright (Warren and Brandeis 1890, p. 201). Nevertheless, the point here is not if privacy be accurately reflected under current copyright statues. Rather, if we view both physical privacy and informational privacy as a kind of property that affords owners access and downstream control rights, then we will have helped to secure the moral status of privacy.

Viewing privacy as a kind of property right may lead us to take privacy more seriously. Loaning my property to someone almost always comes with the implied idea that the property will be returned. When I let you borrow my car, I have not also given consent for you to use my car whenever you desire. Or consider my science fiction novel. Suppose that after years of effort and numerous failures, I come up with a wonderfully entertaining science fiction story. After talking with me about the novel, you ask for a copy, and I gladly oblige. A few weeks later, I am surprised to learn that you have sold my novel to a venture capitalist. My surprise becomes alarm when the plot is substantially changed for a holiday-season movie adaptation you have licensed. In response to my bitter complaints, you reply that by allowing the initial access, I waived all future downstream claims to the work in question.

Setting aside the intuitions surrounding copyright or incentives to produce, we may arguably challenge the default position assumed in this case. The presumption, it would seem, should run the other direction. Allowing access does not entail forfeiting all future downstream claims to physical or intellectual property. If privacy is on a par with physical or intellectual property, then the presumption that access yields forfeiture of future claims should be rejected in the case of private information, as well.

Brain privacy has both physical and informational aspects. In a locational sense, brain privacy would afford individuals the right to control access to their brains or cogitative processes. Whether it is sound waves, electrical impulses, chemicals, or magnetic imaging, there will likely be some technology 'looking into' a specific location or space. Rights to control access to and uses of this specific location would be a form of physical privacy rights. Furthermore, the thoughts, feelings, or preferences that may one day be scanned from a brain are informational in nature. Brain privacy, understood as a subset of a more general right to privacy, would thus include rights over access to and uses of the brain itself, and over the information that may be inferred from scanning.

One worry with this analysis of privacy is that it is overly American and stresses American views and values. I think this worry is unfounded. First, a set of non-relative or culturally-based reasons and arguments have been offered for a specific definition of privacy and for why privacy is morally valuable. If these reasons and arguments are compelling, then they would apply in different contexts.

Second, a case can be made for why the account I have offered fits nicely with at least one EU model of privacy. Richards and Solove note, 'Warren and Brandeis pointed American common law in a new direction, toward a more general protection of "inviolate personality"…[while] English law developed a flexible and powerful law of confidentiality…' (2007, p. 125). It would seem that confidentiality, and the agreements built upon confidentiality, presuppose legitimate prior entitlement or property claims. Imagine Fred steals some personal information from Ginger and then attempts to bind Larry in a confidentiality agreement regarding this information. If there are compelling moral reasons for Larry not to broadcast this information based on a confidentiality agreement, express or implied, they cannot be grounded in Fred's legitimate title. Moreover, by rejecting a 'reasonable expectation of privacy' standard and returning to more of a trespass model, where privacy violations entail trespass on the control of locations or information, I have moved away from what might be called American views of privacy.

Waiving Privacy Rights

While viewing privacy as a form of property may strengthen our commitments, the issue of when privacy may be waived is important (Moore 2016). Let us begin with a relatively mundane case of stepping out for a walk in a public setting. As you enter a public space, you are clearly waiving rights to control access to personal information. Unless you wear a disguise, your height, eye color, gender, and approximate weight and age are all easily accessible. Your words will be heard unless whispered, and your movements will be noticed. It may even be the case that your picture will be taken or there will be a video capture of your walk. Given the way human senses work, it would be odd to maintain that the other inhabitants of the public space should not look at or notice you. Note that you could wear a disguise or walk in public settings where no one else is around—although some governments prohibit using disguises, masks, or other 'identity-hiding' coverings while in public. Minimally, we might claim that by freely entering the public domain, you have waived rights to control access to certain sorts of personal information. However, as already noted, if we view informational privacy rights as similar to intellectual or intangible property rights, we would never conclude that yielding some kinds of access is equivalent to relinquishing all moral claims to the good in question. I do not give up my moral claims to copyright just because I allow you to see my poem.

Consider a different case. In a medical setting, you might justifiably waive access to and control over intimate and deeply personal information about your brain scans. You might even allow your doctor to consult other health-care professionals about your case. None of this seems controversial. However, if a hacker were to access your brain scans and then share them with others, those actions would be access and

use violations. Moreover, if your doctor took your brain scans and shared them with non-medical friends and family there would be access and use violations. Again, waiving access to some bit of personal information is not also to waive control over all downstream uses of this information. It seems our policies and laws simply assume that allowing access is the same as relinquishing all or most rights. I think we should resist this movement.

Consent, Notice, and Control

Outside of cases where individuals clearly waive access claims, such as taking a walk on a busy street or posting a brain scan on the Web, we should insist on norms of consent and notice. For example, if researchers are going to scan your brain while you are playing a game using a virtual reality helmet, your explicit consent should be obtained. If the information found in your brain scans is to be used, saved, or transmitted, consent should also be obtained. Moreover, if your brain scans are to be used in some new way or for a new purpose, again, explicit consent should be obtained. None of this would sound the least bit controversial if we were talking about using your room or your science fiction novel. Legally requiring consent and notice affords individuals an appropriate level of control over their personal information.

Consider the narrower case of employee monitoring. As postulated earlier, suppose we could view your brain at work and discover that you are prejudiced against women, susceptible to depression, or lacking in empathy. Your boss might find such information useful, especially for the purposes of limiting company exposure to lawsuits, lost sales, or theft.

Justifying surveillance of employees in light of privacy rights begins with what I call thin consent (see Moore 2000). A first step in justifying a kind of monitoring is employee notification. The consent takes the following form: 'If your employment is to continue then you must agree to such-and-so kinds of surveillance …' This is appropriately called 'thin consent' because it assumes that jobs are hard to find and the employee in question needs the job. Nevertheless, quitting remains a viable option. An employee cannot consent, even thinly, to surveillance, even brain surveillance, if it is unknown to her. Given a fairly strong presumption in favor of privacy, thin consent would seem obligatory.

It should be clear, however, that thin consent is not enough to justify mandatory employee brain scanning—not in every case. When jobs are scarce, unemployment high, and government assistance programs swamped, thin consent becomes very thin indeed. Under these conditions, employees will be virtually forced to waive privacy rights because of the severe consequences if they do not. But notice what happens when we slide to the other extreme. Assume a condition where there are many more jobs than employees and where changing jobs is relatively easy. In circumstances such as these, thin consent has become quite thick. If employees were to agree to brain scans in these favorable conditions, most would think it justified.

As we slide from one extreme to the other, from a pro-business environment with lots of workers and few jobs to a pro-employee environment with lots of jobs and few workers, this method of justification becomes more plausible. To determine the

exact point where thin consent becomes thick enough to bear the justificatory burden required is a difficult matter. Nevertheless, if the conditions favor the employee, then it becomes plausible to maintain that actual consent would be enough to override a presumption in favor of privacy.

Thick consent is possible when employment conditions minimize the costs of finding a comparable job. What justifies a certain type of surveillance, even brain scanning, is that it *would be agreeable* to a worker in a pro-employee environment. If thin consent is obtained and the test of hypothetical thick consent is met, then we have reason to think that a presumption in favor of privacy has been justifiably surpassed.

Simply by living their lives, individuals create vast amounts of data, and this information is clearly valuable. What else would explain the massive 'information grab' currently practiced by almost every business and government? Admittedly, while managers using various analytical tools add much of the value in these ever-growing data sets, there is value in the raw data itself. The European Union's rules on notice and consent are a welcome step in the right direction:

> [P]ersonal data may be processed only if: (a) the data subject has unambiguously given his consent. (Article 7 of t are a welcome step in the right directDirective No. 46/1996)
>
> [T]he subscriber or user concerned is provided with clear and comprehensive information in accordance with Directive 95/46/EC, inter alia about the purposes of the processing, and is offered the right to refuse such processing by the data controller. (Article 5/3 of Directive No. 58/2002)
>
> Member States shall ensure that the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned has given his or her consent, having been provided with clear and comprehensive information, in accordance with Directive 95/46/EC, inter alia, about the purposes of the processing by the data controller. (Directive No. 2009/136/EC)

If there were few exceptions, requiring prior consent and notice of use would go a long way toward protecting individual privacy rights in general and brain privacy in particular. But even in the EU, there are numerous exceptions that allow companies and governments to use, transfer, and control personal information without notice or consent. For example, if the 'processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller', then use may be legitimate without consent or notice (EU Directive 95/46/EC—The Data Protection Directive). Imagine that linking individual brain scans with other large data sets allowed predictive analytic engines to determine whether someone is likely to commit a crime. Perhaps unlike the rest of us, some individuals are more likely to commit crimes. In such cases, the 'public interest' in preventing crime may be invoked to override rules on consent and notice even though these individuals may never commit a crime.

Probable Cause

In US Fourth Amendment law, probable cause forms the boundaries of acceptable state intrusion into private affairs. It prevents the state from engaging in 'fishing expeditions', and limits state action to situations in which officers have a reasonable basis to believe criminal activity has occurred. If an agent of the government can demonstrate that a target has committed, is committing, or will commit a crime, then an independent authority, such as a judge, can issue a warrant or subpoena (Moore 2011, 2016).

With probable cause, a warrant issued from a judge, and sunlight provisions opening up the warrant and the procedure to public scrutiny, we can be confident that security or public interest concerns may be addressed with minimal impact on individual privacy. The probable-cause requirement puts the burden of proof in the appropriate place; invasions of private domains must be justified. The official seeking the warrant would highlight the values involved, along with the privacy interests at stake. Judicial oversight inserts an outside element into the process, providing a check on the enthusiasm of law enforcement officials.

Obviously, I am staunchly opposed to what is known as the 'third party doctrine' in the US. According to this doctrine, by voluntarily giving information to third parties, such as phone companies, Internet providers, or banks, individuals relinquish privacy claims and have no 'reasonable expectation of privacy' concerning this information. Worse yet, because there is no expectation of privacy, government agents can access this information without a court order. There is no need to apply for a warrant or show probable cause. Because of the third party doctrine, over the past decade there has been an alarming decrease in applications for warrants and a sharp increase in the use of subpoenas (Slobogin 2005).

Related to brain privacy or neuro-surveillance, both physical and informational, I would argue that warrants should be the standard. If a government agent can provide compelling evidence of criminal activity and that access to a suspect's brain scan records is necessary for a criminal investigation, then a warrant should be issued and a search conducted. Access to these documents on a third party server would be excluded without a warrant. Moreover, if access is allowed because a warrant has been issued, the rule of notice should still be followed. The information target should be notified that his or her brain scan information has been accessed by law enforcement.

Conclusion

In 1761 James Otis (1761) noted the long English tradition of 'a man's house is his castle'. Likewise, addressing the English Parliament, William Pitt wrote, 'The poorest man may in his cottage bid defiance to all the force of the crown. It may be frail—its roof may shake—the wind may blow through it—the storm may enter, the rain may enter—but the King of England cannot enter—all his force dares not cross the threshold of the ruined tenement" (1763, p. 52). I would argue that the strength of these sentiments should be applied to neuro-privacy, as well. Allowing limited

access to brain scans for specific purposes is not also a license that allows others unfettered access to, or use of, this information. If crossing into the private domain of a person's house requires robust justification, then it would seem a similar justification should be offered to peer into the human mind.

By viewing privacy as a kind of property while being mindful of the distinction between access and use, we may more easily apply the privacy-protecting principles of consent, notice, and probable cause related to neuro-surveillance. Consider a different area of privacy. Decisional privacy in the US began with the idea that there was no compelling state interest in prohibiting contraceptive use between spouses and ended in a woman's right to choose. In *Roe v. Wade*, Justice Blackmun (1973) argued that '[t]he right to privacy, whether it be founded in the Fourteenth Amendment's concept of personal liberty and restrictions upon the state action, as we feel it is, or, as the District Court determined, in the Ninth Amendment's reservation of rights to the people, is broad enough to encompass a woman's decision whether or not to terminate her pregnancy.' A woman's right to control access to and uses of her own body, and the right to make decisions about access and use, is central to the area of decisional privacy. We would never countenance interference in this domain without a weighty and compelling justification. Viewing brain privacy in a similar light casts moral aspersions on the practice of neuro-surveillance and the host of coming technologies that promise to peer into the sanctity of the human mind.

References

Allen, Anita. 2003. *Why privacy isn't everything: Feminist reflections on personal accountability*. Lanham, MD: Rowman and Littlefield.

Allen, Anita. 2008. The virtuous spy: Privacy as an ethical limit. *The Monist* 91: 3–22.

Allen, Anita. 2011. *Unpopular privacy: What must we hide?*. Oxford: Oxford University Press.

Barnes, Grace M., Michael P. Farrell, and Sarbani Banerjee. 1994. Family influences on alcohol abuse and other problem behaviors among black and white adolescents in a general population sample. *Journal of Research on Adolescence* 4: 183–201.

Baum, Andrew, and Stuart Koman. 1976. Differential response to anticipated crowding: Psychological effects of social and spatial density. *Journal of Personality and Social Psychology* 34: 526–536.

Benn, S.I., and Gerald F. Gaus. 1983. *Public and private in social life*. New York, NY: St. Martin's Press.

Blackmun, Harry. 1973. *Roe v. Wade*, U.S. 410(153):164–165.

Bonaci, Tamara, Ryan Calo, and Howard Jay Chizeck. 2014. App stores for the brain: Privacy & security in brain–computer interfaces. In *2014 IEEE International Symposium on Ethics in Science, Technology and Engineering*. 1–7, 23–24.

Chekroud Adam M., Jim A. C. Everett, Holly Bridge, and Miles Hewstone. 2014. A review of neuroimaging studies of race-related prejudice: Does amygdala response reflect threat? *Frontiers in Human Neuroscience*. 8. http://journal.frontiersin.org/article/10.3389/fnhum.2014.00179/full#B60.

Clauson-Kaas, J., A. Dzikus, C. Stephens, N. Hojlyng, and P. Aaby. 1996. Urban health: Human settlement indicators of crowding. *Third World Planning Review* 18: 349–363.

Cox, Verne C., Paul B. Paulus, and Garvin McCain. 1984. Prison crowding research: The relevance of prison housing standards and a general approach regarding crowding phenomena. *American Psychologist* 39: 1148–1160.

Cyranoski, David. 2012. Neuroscience: The mind reader. http://www.nature.com/news/neuroscience-the-mind-reader-1.10816.

Davis, Frederick. 1959. What do we mean by 'Right to privacy'? *South Dakota Law Review* 4: 1–24.

DeCew, Judith W. 1997. *In pursuit of privacy: Law, ethics, and the rise of technology*. Ithaca, NY: Cornell University Press.

Douglas, William O. 1966. *Osborn v. United States*, 385 U.S. 323.

Eaton, Nicholas, Robert F. Kruger, Wendy Johnson, Matt McGue, and William G. Iacono. 2009. Parental monitoring, personality, and delinquency: Further support for a reconceptualization of monitoring. *Journal of Research in Personality* 43: 49–59.

Edwards, John N., and Alan Booth. 1977. Crowding and human sexual behavior. *Social Forces* 55: 791–808.

Erikson, Erik H. 1963. *Childhood and society*. New York, NY: Norton.

Farah, Martha J. 2011. Neuroscience and neuroethics in the 21st century. In *The Oxford handbook of neuroethics*, ed. Judy Illes, and Barbara J. Sahakian. Oxford: Oxford University Press.

Farah, Martha J., Elizabeth M. Smith, Cyrena Gawuga, Dennis Lindsell, and Dean Foster. 2008. Brain imaging and brain privacy: A realistic concern? *Journal of Cognitive Neuroscience*. 21(1).

Farahany, Nita. 2012. Incriminating thoughts. *Stanford Law Review*. 64.

Farrington, David P., and Christopher P. Nuttall. 1980. Prison size, overcrowding, prison violence and recidivism. *Journal of Criminal Justice.* 8: 221–231.

Federspiel, William. 2008. 1984 Arrives: Thought (crime), technology, and the constitution. *William and Mary Bill of Rights Journal*. 16.

Finn, David. 2006. Brain imaging and privacy: How recent advances in neuroimaging implicate privacy concerns. *Bepress Legal Series*. Working paper 1752.

Fischbach, Ruth, and Janet Mindes. 2011. Why neuroethicists are needed. In *The Oxford handbook of neuroethics*, ed. Judy Illes, and Barbara J. Sahakian. Oxford: Oxford University Press.

Fuller, Theodore D., John N. Edwards, Sairudee Vorakitphokatorn, and Santhat Sermsri. 1996. Chronic stress and psychological well-being: evidence from Thailand on household crowding. *Social Science Medicine* 42: 265–280.

Gavison, Ruth. 1983. Information control: Availability and control. In *Public and private in social life*, ed. S. Benn, and G. Gaus, 113–134. New York, NY: St. Martin's Press.

Gligorov, Nada, and Stephen C. Krieger. 2010. Functional neuroimaging, free will, and privacy. In *Healthcare and the effect of technology: developments, challenges and advancements*, ed. Stéfane M. Kabene. Hershey, PA: Medical Information Science Reference.

Gross, Hyman. 1971. Privacy and autonomy. In *Privacy*, ed. John W. Chapman, and J. Roland Pennock, 169–181. New York, NY: Atherton Press.

Hallinan, Dara, Michael Friedewald, Philip Schütz, and Paul de Hert. 2014. Neurodata and neuroprivacy: Data protection outdated? *Surveillance and Society* 12(1): 55–72.

Hare, Amanda L., Emily G. Marston, and Joseph P. Allen. 2011. Maternal acceptance and adolescents' emotional communication: A longitudinal study. *Journal of Youth and Adolescence* 40: 744–751.

Hart, Allen J., Paul J. Whalen, Lisa M. Shin, Sean C. McInerney, Hakan Fischer, and L. Scott. 2000. Differential response in the human amygdala to racial outgroup vs ingroup face stimuli. *NeuroReport* 11: 2351–2355.

Haynes, John-Dylan. 2012. Brain reading. In *I know what you're thinking: Brain imaging and mental privacy*, ed. Sarah Richmond, Geraint Rees, and Sarah J. L. Edwards. Oxford: Oxford University Press.

Hobbes, Thomas. 1985. Leviathan: 1651. In *Penguin Classics*, ed. C. B. MacPhereson

Kafka, Randy, and Perry London. 1991. Communication in relationships and adolescent substance use: The influence of parents and friends. *Adolescence* 26: 587–598.

Kerr, Margaret, and Hakan Stattin. 2000. What parents know, how they know it, and several forms of adolescent adjustment: Further support for a reinterpretation of monitoring. *Journal of Developmental Psychology.* 36: 366–380.

Kessler, Jane. 1966. *Psychopathology of childhood.* Englewood Cliffs, NJ: Prentice-Hall.

Laudon, Kenneth. 1996. Markets and privacy. *Communications of the ACM* 39: 93–104.

Lessig, Lawrence. 2002. Privacy as property. *Social Research* 69: 247–269.

Lever, Annabelle. 2016. Democracy, privacy, and security. In *Privacy, security, and accountability*, ed. Adam D. Moore. Lanham, MD: Rowman and Littlefield International.

Lever, Annabelle. 2012. Neuroscience v. privacy? A democratic perspective. In *I know what you're thinking: Brain imaging and mental privacy*, ed. S. Richmond, G. Rees, and S. J. L. Edwards. Oxford: Oxford University Press.

Lewis, Tanya. 2013. Brain says guilty! Neural imaging may nab criminals. http://www.livescience.com/37091-brain-imaging-in-the-courtroom.html.

Martinovic, Ivan, Doug Davies, Mario Frank, Daniele Perito, Tomas Ros, and Dawn Song. 2012. On the feasibility of side-channel attacks with brain-computer interfaces. In *Proceedings of the 21st USENIX conference on security symposium*. Berkeley, CA: USENIX Association.

McCain, Garvin, Verne Cox, and Paul B. Paulus. 1980. *The effect of prison crowding on inmate behavior*. Washington DC: US Department of Justice.

McGinley, Phyllis McGinley. 1959. *A lost privilege. Province of the heart*. New York, NY: Viking Press.

Megargee, Edwin. 1977. The association of population density reduced space and uncomfortable temperatures with misconduct in a prison community. *The American Journal of Community Psychology* 5: 289–298.

Mill, John Stuart, 1859. *On Liberty*. London: Longman, Roberts & Green.

Miller, Greg. 2014. Scientists can't read your mind with brain scans (yet). http://www.wired.com/2014/04/brain-scan-mind-reading/.

Moore, Adam D. 2000. Employee monitoring & computer technology: Evaluative surveillance v. privacy. *Business Ethics Quarterly* 10(3): 697–709.

Moore, Adam D. 2001. *Intellectual property and information control: Philosophic foundations and contemporary issues*. New Brunswick, NJ: Transaction Publishers.

Moore, Adam D. 2003. Privacy: Its meaning and value. *American Philosophical Quarterly* 40: 215–227.

Moore, Adam D. 2007. Toward informational privacy rights. *San Diego Law Review* 44: 809–845.

Moore, Adam D. 2008. Defining Privacy. *Journal of Social Philosophy* 39: 411–428.

Moore, Adam D. 2010. *Privacy rights: Moral and legal foundations*. University Park, PA: Penn State University Press.

Moore, Adam D. 2011. Privacy, security, and government surveillance: Wikileaks and the new accountability. *Public Affairs Quarterly*. 25.

Moore, Adam D. 2016. *Waiving privacy rights: Responsibility, paternalism, and liberty*. Forthcoming, Brookings Institute Press. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2673717.

Moreno, Jonathan D. 2011. Brain trust: neuroscience and national security in the 21st century. In *The Oxford handbook of neuroethics*, ed. Judy Illes, and Barbara J. Sahakian. Oxford: Oxford University Press.

Morgan, Griscom. 1972. Mental and social health and population density. *Journal of Human Relations* 20: 196–204.

Mumford, Lewis. 1961. *The city in history*. New York, NY: Harcourt Brace.

Murdock, George P. 1955. The universals of culture. In *Readings in world anthropology*, ed. E. Adamson Hoebel, Jesse D. Jennings, and Elmer R. Smith. New York, NY: McGraw-Hill.

Murphy, Emily R., and Henry T. Greely. 2011. What will be the limits of neuroscience-based mindreading in the law? In *The Oxford handbook of neuroethics*, ed. Judy Illes, and Barbara J. Sahakian. Oxford: Oxford University Press.

Newell, Bryce, Cheryl Metoyer, and Adam D. Moore. 2015. Privacy in the family. In *The social dimensions of privacy*, ed. Beate Roessler, and Dorota Mokrosinska. Cambridge: Cambridge University Press.

Nissenbaum, Helen. 2009. *Privacy in context: Technology, policy, and the integrity of social life*. Stanford, CA: Stanford University Press.

Nissenbaum, Helen, and Finn Brunton. 2015. *Obfuscation: A user's guide for privacy and protest*. Cambridge, MA: MIT Press.

Nussbaum, Martha C. 2000. *Woman and human development: The capabilities approach*. Cambridge: Cambridge University Press.

Otis, James. 1761. In O*pposition to writs of assistance. Delivered before the Superior Court*. Boston, MA.

Parent, W. A. 1983. Privacy, morality, and the law. *Philosophy and Public Affairs* 12: 269–288.

Parker, Richard B. 1974. A definition of privacy. *Rutgers Law Review* 27: 275–296.

Paulus, Paul B., Verne C. Cox, and Garvin McCain. 1978. Death rates, psychiatric commitments, blood pressure and perceived crowding as a function of institutional crowding. *Environmental Psychology and Nonverbal Behavior* 3: 107–116.

Pennock, J. Roland, and John W. Chapman. 1971. *Privacy: Nomos XIII*. New York, NY: Atherton Press.

Phelps, Elizabeth A., Kevin J. O'Connor, William A. Cunningham, E. Sumie Funayama, J. Christopher Gatenby, John C. Gore, and Mahzarin R. Banaji. 2000. Performance on indirect measures of race evaluation predicts amygdala activation. *Journal of Cognitive Neuroscience* 12: 729–738.

Pitt, William (the elder, Earl of Chatham). 1763. Speech in the House of Lords. In *Historical sketches of statesmen who flourished in the time of George III,* vol. 1, by Henry Peter Brougham (London and Glasgow: R. Griffin and Co., 1839).

Porporino, F. J., and K. Dudley. 1984. *An analysis of the effects of overcrowding in Canadian penitentiaries*. Ottawa: Research Division, Programs Branch, Solicitor General of Canada.

Rachels, James. 1975. Why privacy is important. *Philosophy and Public Affairs* 4: 323–333.

Richards, Neil, and Daniel Solove. 2007. Privacy's other path: Recovering the law of confidentiality. *The Georgetown Law Journal* 96: 123–182.

Richmond, Sara, Geraint Rees, and Sarah J. L. Edwards. 2012. *I know what you're thinking: Brain imaging and mental privacy*. Oxford: Oxford University Press.

Roberts, John M., and Thomas Gregor. 1971. Privacy: A cultural view. In *Privacy*, ed. J. Roland Pennock and John W. Chapman, 199–225. New York, NY: Atherton Press.

Rossiter, Clinton. 1958. *Aspects of liberty*. Ithaca: Cornell University Press.

Rössler, B. 2005. *The value of privacy* (trans. by Rupert, D. V.). Glasgow and Cambridge, UK: Polity.

Ruback, R. Barry, and Timothy S. Carr. 1984. Crowding in a woman's prison. *Journal of Applied Social Psychology* 14: 57–68.

Samuelson, Pamela. 2000. Privacy as intellectual property? *Stanford Law Review.* 52: 1125–1173.

Schoeman, Ferdinand David. 1992. *Privacy and social freedom*. New York, NY: Cambridge University Press.

Schwartz, Barry. 1968. The social psychology of privacy. *American Journal of Sociology* 73: 741–752.

Slobogin, Christopher. 2005. Subpoenas and privacy. *DePaul Law Review* 54: 805.

Spiro, Herbert J. 1971. Privacy in comparative perspective. In *Privacy*, ed. J. Roland Pennock and John W. Chapman, 121–148. New York, NY: Atherton Press.

Spitz, Rene A. 1964. The derailment of dialogue. *Journal of the American Psychoanalytic Association* 12: 752–775.

Stattin, Hakan, and Margaret Kerr. 2000. Parental monitoring: A reinterpretation. *Child Development* 71: 1072–1085.

Thomson, Judith Jarvis. 1975. The right to privacy. *Philosophy and Public Affairs* 4: 295–314.

Warren, Samuel D., and Louis Brandeis. 1890. The right to privacy. *The Harvard Law Review* 4: 193–220.

Westin, Alan. 1967. *Privacy and freedom*. New York, NY: Atheneum.