Toward Informational Privacy Rights†

ADAM D. MOORE*

TABLE OF CONTENTS

† An early version of this paper was presented at the 2005 Pacific Division Meetings of the American Philosophical Association and the Mini-Conference on Security, March 2006. Thanks to Judith Wagner DeCew, Ken Himma, and the other session participants for their suggestions. I would like to thank Kim Moore and those who participated in the University of San Diego Institute for Law and Philosophy 2007 Editors' Symposium *Informational Privacy: Philosophical Foundations and Legal Implications*, James P. Griffin, Ken Himma, Daniel J. Solove, Amitai Etzioni, David Brink, Steve Smith, Samuel C. Rickless, Alan Rubel, Adam Kolber, and Evan Tsen Lee, for providing helpful comments and analysis. Finally, I would like to thank Amanda Fitzsimmons, Maria Stout, and the other editors at the *San Diego Law Review* for their help and assistance in preparing this paper for publication.

* Associate Professor, University of Washington. Professor Moore holds a joint appointment in the Philosophy Department and the Information School.

Advancements in information technologies promise to make our lives transparent.[1] Corporations large and small engage in data mining activities that capture massive amounts of information. Much of this mined information is about our daily activities—what was purchased, where, and for how much. Our mailboxes and e-mail accounts are then stuffed with an endless stream of advertisements and solicitations. Even more alarming are telemarketers who intrude upon our solitude at home. Financial information, phone numbers, and personal addresses of all sorts, whether accurate or not, are captured in databases and bought and sold to individuals, corporations, and government agencies. Beyond data mining, video surveillance, facial recognition technology, and spyware, a host of other invasive tools are opening up private lives for public consumption.[2]

Advocates of informational privacy are opposed to a system that promotes the free flow of personal information, driven more or less by economic considerations and national security interests. Many privacy supporters have welcomed the European Union's statutory regulations regarding personal data storage and transfer. And while the United States protects informational privacy, it is arguably the case that these protections are fairly weak[3]—or at least not as strong as the European Privacy Directive.[4]

In this paper I will offer several arguments in support of the view that individuals have moral claims to control personal information. Coupled with rights to control access to one's body, capacities, and powers, or physical privacy rights, we will have taken important steps toward a general right to privacy. In Part I, a definition of privacy is offered

1. *See generally* DAVID BRIN, THE TRANSPARENT SOCIETY (1998) (discussing how technology diminishes privacy).

2. According to one estimate there are more than four million surveillance cameras in Britain. JEFFERY ROSEN, THE NAKED CROWD 36 (2004), *citing* Michael McCahill & Clive Norris, *CCTV in London* 20 (Urbaneye Working Paper No. 6, 2002), http://www.urbaneye.net/results/ue_wp6.pdf.

3. *See* JUDITH WAGNER DECEW, IN PURSUIT OF PRIVACY: LAW, ETHICS, AND THE RISE OF TECHNOLOGY 148–51 (1997); Randal Kemp & Adam D. Moore, *Privacy*, 25 LIBR. HI TECH 58, 67–72 (2007).

4. Council Directive 95/46/EC, 1995 O.J. (L 281) 31, *available at* http://ec.europa.eu/justice_home/fsj/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf and http://ec.europoa.eu/justice_home/fsj/privacy/docs/95-46-ce/dir1995-46_part2_en.pdf.

along with an account of the value of privacy. Simply put, privacy—defined as control over access to locations and information—is necessary for human well-being. In Part II, an attempt to move beyond claims of value to claims of obligation is presented and defended. Policies that sanction the capturing, storing, and trading of personal information about others is something we each have reasons to avoid. In the final part, the tension between privacy and security is considered. It is argued that privacy rights may be set aside only if specific procedural conditions are followed.

I. PRIVACY: ITS MEANING AND VALUE[5]

A. The Meaning of Privacy

Privacy has been defined in many ways over the last century.[6] Samuel D. Warren and Louis D. Brandeis, following Judge Thomas Cooley, called privacy "the right to be let alone."[7] Roscoe Pound and Paul A. Freund have defined privacy in terms of an extension of one's personality or personhood.[8] Legal scholar William Prosser separated privacy cases into four related torts: intrusion, private facts, false light, and appropriation.[9] These torts have been defined as follows:

> *Intrusion*: Intruding (physically or otherwise) upon the solitude of another in a highly offensive manner. . . . *Private facts*: Publicizing highly offensive private information about someone which is not of legitimate concern to the public. . . . *False light*: Publicizing a highly offensive and false impression of another. . . . *Appropriation*: Using another's name or likeness for some advantage without the other's consent.[10]

---

5. Some of this part draws from Adam D. Moore, *Privacy: Its Meaning and Value*, 40 AM. PHIL. Q. 215, 215–23 (2003).

6. *See* DECEW, *supra* note 3, chs. 1–4 (providing rigorous analysis of the major accounts of privacy that have been offered); Kemp & Moore, *supra* note 3, at 62–66. *See generally* Daniel Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477 (2006) (attempting to delineate privacy's bounds by discussing a "taxonomy" of activities that harm privacy).

7. *See* THOMAS M. COOLEY, A TREATISE ON THE LAW OF TORTS 29 (2d ed. 1888); Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 195 (1890).

8. *See* Paul A. Freund, *Privacy: One Concept or Many*, *in* NOMOS XIII: PRIVACY 182, 182–84 (J. Roland Pennock & John W. Chapman eds., 1971); Roscoe Pound, *Interests in Personality*, 28 HARV. L. REV. 343, 362–64 (1915).

9. William L. Prosser, *Privacy*, 48 CAL. L. REV. 383, 389 (1960).

10. ELLEN ALDERMAN & CAROLINE KENNEDY, THE RIGHT TO PRIVACY 155–56 (1995).

Alan Westin and others, including myself, have described privacy in terms of information control.[11] Still others have insisted that privacy consists in the form of autonomy over personal matters.[12] William Parent argued, "Privacy is the condition of not having undocumented personal knowledge about one possessed by others,"[13] while Julie Inness defined privacy as "the state of possessing control over a realm of intimate decisions, which includes decisions about intimate access, intimate information, and intimate actions."[14] More recently, Judith Wagner DeCew has proposed the "realm of the private to be whatever is not, according to a reasonable person in normal circumstances, the legitimate concern of others."[15] This brief summary indicates the variety and breadth of the definitions that have been offered.[16]

I favor what has been called a control-based definition of privacy. That is, privacy has to do with control over access to oneself and to information about oneself.[17] One feature of such a conception is that it can incorporate much of the aforementioned definitions. Controlling

---

11. ADAM D. MOORE, INTELLECTUAL PROPERTY AND INFORMATION CONTROL 181–82 (2001); ALAN F. WESTIN, PRIVACY AND FREEDOM 7 (1967); *see also* ANITA L. ALLEN, WHY PRIVACY ISN'T EVERYTHING: FEMINIST REFLECTIONS ON PERSONAL ACCOUNTABILITY 115–16 (2003). *See generally* Ruth Gavison, *Information Control: Availability and Exclusion*, *in* PUBLIC AND PRIVATE IN SOCIAL LIFE 113 (S.I. Benn & G.F. Gaus eds., 1983) (discussing the distinction between public and private information, conflicts over information controls, and possible resolutions for information-control conflicts).

12. *See* Eisenstadt v. Baird, 405 U.S. 438, 453 (1972); *see also* H. Tristram Engelhardt, Jr., *Privacy and Limited Democracy: The Moral Centrality of Persons*, SOC. PHIL. & POL'Y, Summer 2000, at 120, 123–24; Joel Feinberg, *Autonomy, Sovereignty, and Privacy: Moral Ideals in the Constitution?*, 58 NOTRE DAME L. REV. 445, 446 (1983); Louis Henkin, *Privacy and Autonomy*, 74 COLUM. L. REV. 1410, 1410–11 (1974); Daniel R. Ortiz, *Privacy, Autonomy, and Consent*, 12 HARV. J.L. & PUB. POL'Y 91, 91–92 (1989).

13. W.A. Parent, *Privacy, Morality, and the Law*, 12 PHIL. & PUB. AFF. 269, 269 (1983).

14. JULIE C. INNESS, PRIVACY, INTIMACY, AND ISOLATION 140 (1992).

15. DECEW, *supra* note 3, at 62.

16. Samuel Rickless offers a barrier theory of privacy: "For *X* to have a right to privacy against *Y* is for *X* to have a claim against *Y* that *Y* not learn or experience some personal fact about *X* by breaching a barrier used by *X* to keep others from learning or experiencing some personal fact about *X*." Samuel C. Rickless, *The Right to Privacy Unveiled*, 44 SAN DIEGO L. REV. 773, 787 (2007). One problem with this account is that it is not at all clear what counts as breaching a barrier. A bad disguise might be a barrier to those with poor eyesight while walls, fences, and security systems may not be a barrier to someone with Superman ears.

17. *See also* ALLEN, *supra* note 11, at 1–2; CHARLES FRIED, AN ANATOMY OF VALUES: PROBLEMS OF PERSONAL AND SOCIAL CHOICE 140–41 (1970); Gavison, *supra* note 11, at 113–20, 129–32; Hyman Gross, *Privacy and Autonomy*, *in* NOMOS XIII: PRIVACY, *supra* note 8, at 169, 170; Richard B. Parker, *A Definition of Privacy*, 27 RUTGERS L. REV. 275, 279–80 (1974); Ernest Van Den Haag, *On Privacy*, *in* NOMOS XIII: PRIVACY, *supra*, at 149, 149; Richard Wasserstrom, *Privacy: Some Arguments and Assumptions*, *in* PHILOSOPHICAL LAW 148, 148 (Richard Bronaugh ed., 1978).

access to ourselves affords individuals the space to develop as they see fit. Such control yields room to grow personally while maintaining autonomy over the course and direction of one's life. Moreover, each of Prosser's torts contains elements of access control. Also, note that there is room for the distinction between physical privacy and informational privacy. The former would afford individuals a right to control access to their bodies and places, while the latter yields a right to control access to personal information, no matter how it is instantiated.

A serviceable notion of personal information comes from William Parent: "My suggestion is that it be understood to consist of *facts* about a person which . . . individuals in a given society at a given time do not want widely known about themselves."[18] More generally, personal information might be loosely defined as information or facts about specific individuals rather than inanimate objects, social institutions, and the like.[19] 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.[20]

In addition to the different conceptions already noted, there are two distinctions relating to the definition of privacy that have been widely discussed. 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 is Parent's definition: "Privacy is the *condition* of not having undocumented personal knowledge about one possessed by others."[21] A normative account, on the other hand, makes references to moral obligations or claims. For example, when DeCew talks about what is a "legitimate concern of others," she includes ethical considerations.[22]

---

18. Parent, *supra* note 13, at 269–70 (citation omitted).

19. As with *privacy*, defining the term *information* is difficult. *See, e.g.*, Michael K. Buckland, *Information as Thing*, 42 J. AM. SOC'Y INFO. SCI. 351 (1991); C.E. Shannon, *A Mathematical Theory of Communication*, 27 BELL SYS. TECH. J. 379 (1948); Andrzej Chmielecki, *What is Information?*, TWENTIETH WORLD CONGRESS OF PHILOSOPHY, Aug. 1998, http://www.bu.edu/wcp/Papers/Cogn/CognChmi.htm.

20. On this view, just because some bit of information is publicly available does not mean that it is not personal information.

21. Parent, *supra* note 13, at 269 (emphasis added).

22. DECEW, *supra* note 3, at 57–58. Many counterexamples to control-based definitions of privacy illicitly move back and forth between non-normative and normative conceptions. For example, Rickless, following Parent's example, describes the Threatened

Reductionist and nonreductionist accounts of privacy have also been offered.[23] Reductivists 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. Viewing privacy in this fashion might mean jettisoning the idea altogether and focusing on more fundamental concepts. For example, Frederick Davis has argued:

> If 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.[24]

Unlike Davis, the nonreductionist views privacy as related to, but distinct from, other rights or concepts.

These distinctions are not as important as some may have thought. First, it is possible and proper to define privacy along normative and descriptive dimensions. Intellectual property is also defined descriptively and normatively. We may, for example, define intellectual property without making any essential references to normative claims. We can even give a description of the conditions that surround an intellectual property right. Moreover, we can define intellectual property in normative terms by indicating the moral claims that surround persons and their property. The same is true of privacy.

Second, without considering the justification of the rights involved, it is unclear if privacy is reducible to more basic rights or the other way around. Parent and others have made this point.[25] 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.

Loss Counterexample, which has no force if we are considering a *right* to control access. *See* Rickless, *supra* note 16, at 782–84.

23. For an analysis of the reductive versus nonreductive debate, see generally Amy Peikoff, *No Corn on this Cobb: Why Reductionists Should Be All Ears for* Pavesich, 42 BRANDEIS L.J. 751 (2004). *See also* Judith Jarvis Thomson, *The Right to Privacy*, 4 PHIL. & PUB. AFF. 295, 304–05 n.4 (1975). For a critique of Thomson's view of privacy, see Thomas Scanlon, *Thomson on Privacy*, 4 PHIL. & PUB. AFF. 315 (1975).

24. Frederick Davis, *What Do We Mean by "Right to Privacy"?*, 4 S.D. L. REV. 1, 20 (1959).

25. *See* DECEW, *supra* note 3, at 29 (citing Jeffrey Reiman, *Privacy, Intimacy, and Personhood*, 6 PHIL. & PUB. AFF. 26–44 (1976); Scanlon, *supra* note 23, at 315–22.

B. The Value of Privacy

While privacy rights may entail obligations and claims against others, obligations and claims that are beyond the capacities of most nonhuman animals, a case can still be offered in support of the claim that separation is valuable for animals. Even though privacy may be linked to free will, the need for separation provides an evolutionary first step. Perhaps it is the capacity of freewill that changes mere separation into privacy. Alan Westin notes in *Privacy and Freedom*:

> 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.[26]

More important 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. Lemmings may march into the sea or there may be what is called a "biochemical die-off." John J. Christian's study of a herd of Sika deer illustrates the point: "Mortality evidently resulted from shock following severe metabolic disturbances, probably as a result of prolonged adrenocortical hyperactivity, judging from histological material. There was no evidence of infection, starvation, or other obvious cause to explain the mass mortality."[27] In this case the inability to separate from other members of the same species apparently caused a die-off so that herd numbers could accommodate separation.[28]

John Calhoun notes that experiments with rats and spacing in cages show that a certain level of separation is necessary for the species.[29] The lack of separation leads to the disruption of social relationships and increases in disease, high blood pressure, and heart failure. Calhoun allowed Norway rats, which were amply fed, to breed freely in a quarter-acre pen. Their numbers stabilized at 150 and never exceeded 200.[30] With a

---

26. WESTIN, *supra* note 11, at 8.
27. John J. Christian, *Phenomena Associated with Population Density*, 47 PROC. NAT'L ACAD. SCI. 428, 444 (1961).
28. *Id.* at 443–46.
29. Edward T. Hall, *Proxemics*, 9 CURRENT ANTHROPOLOGY 83, 87 (1968) (citing John B. Calhoun, *The Study of Wild Animals Under Controlled Conditions*, 51 ANNALS N.Y. ACAD. SCI. 1113–15 (1950)).
30. *Id.*

population of 150, fighting became so disruptive to normal maternal care that only a few of the young survived. If placed in pens, the same area could support 5,000 rats.[31] Moreover these results hold across a wide range of species, supporting the contention that separation, like food and water, is a necessity of life.[32]

If it is plausible to maintain that humans evolved from nonhuman animals, then it is also plausible that humans may retain many of the same traits. The question now becomes, is separation a necessity for well-being, and is it found in human cultures? If so, like other basic requirements for living, we may plausibly conclude that privacy is valuable.

Cultural universals have been found in every society that has been systematically studied.[33] Based on the Human Relations Area Files at Yale University, Alan F. Westin argues that there are aspects of privacy found in every society—privacy *is* a cultural universal.[34]

Barry Schwartz, in an important article dealing with the social psychology of privacy, provides interesting clues as to why privacy is universal.[35] According to Schwartz, privacy is both group preservation

---

31. WESTIN, *supra* note 11, at 10; *see also* W.C. ALLEE, THE SOCIAL LIFE OF ANIMALS 91 (1938) (finding that overcrowding reduces growth in animal species); ROBERT ARDREY, THE TERRITORIAL IMPERATIVE 55–56 (1966) (discussing animal territoriality and its effect on reproductive success); John B. Calhoun, *A Behavorial Sink*, *in* ROOTS OF BEHAVIOR 295, 314–15 (Eugene L. Bliss ed., 1962) (discussing rat overcrowding experiment that led to atypical behavior and reproductive failure); John B. Calhoun, *Population Density and Social Pathology*, 206 SCI. AM. 139, 139 (1962) (same); EDWARD T. HALL, THE HIDDEN DIMENSION 23 (Anchor Books 1982) (1966); H. ELLIOT HOWARD, TERRITORY IN BIRD LIFE 273–75 (reprint 1978) (1920) (describing territoriality among bird species).

32. *See, e.g.*, ALLEE, *supra* note 31, at 91; V.C. WYNNE-EDWARDS, ANIMAL DISPERSION IN RELATION TO SOCIAL BEHAVIOUR 188–89 (1962); Edward S. Deevey, *The Hare and the Haruspex: A Cautionary Tale*, 49 YALE REV. 161, 178 (1959), *reprinted in* 48 AM. SCI. 415 (1960); E. Thomas Gilliard, *On the Breeding Behavior of the Cock-of-the-Rock (Aves, Rupicola rupicola)*, 124 BULL. AM. MUSEUM NAT'L HIST. 31, 61–63 (1963); Robert L. Snyder, *Evolution and Integration of Mechanisms that Regulate Population Growth*, 47 PROC. NAT'L ACAD. SCI. 449, 454 (1961).

33. *See* George P. Murdock, *Universals of Culture*, *in* READINGS IN ANTHROPOLOGY 4 (E. Adamson Hoebel et al. eds., 1955).

34. WESTIN, *supra* note 11, at 12–13. John Roberts and Thomas Gregor support this view of privacy:

> [P]rivacy as a set of rules against intrusion and surveillance focused on the household occupied by a nuclear family is a conception which is not to be found universally in all societies. *Societies stemming from quite different cultural traditions such as the Mehinacu and the Zuni do not lack rules and barriers restricting the flow of information within the community, but the management and the functions of privacy may be quite different.*

John M. Roberts & Thomas Gregor, *Privacy: A Cultural View*, *in* NOMOS XIII: PRIVACY, *supra* note 8, at 199, 225 (emphasis added).

35. Barry Schwartz, *The Social Psychology of Privacy*, 73 AM. J. SOC. 741, 741–52 (1968).

and maintenance of status divisions, but it also allows for deviation while sustaining social establishments.[36] As such, privacy may be woven into the fabric of human evolution.

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.[37] 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. As with the necessities of food, shelter, and education, we should not jump to the conclusion that because the forms of privacy are culturally dependent, privacy is subjective "all the way down." The forms of privacy are culturally relational while the need is an objective necessity.

In 1969, Edward Hall noted a link between a lack of privacy and psychological and physical disorders in humans and nonhuman animals.

> The disorders of Calhoun's overcrowded rats bear a striking resemblance to . . . Americans who live in densely packed urban conditions. . . . Chombart de Lauwe . . . has gathered data on French workers' families and has demonstrated a statistical relationship between crowded living conditions and physical and social pathology. In the United States a health survey of Manhattan showed that only 18% of a representative sample were free of emotional disorders while 23% were seriously disturbed or incapacitated.[38]

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 Megapolis.[39]

---

36. *Id.*

37. *See* Herbert J. Spiro, *Privacy in Comparative Perspective*, *in* NOMOS XIII: PRIVACY, *supra* note 8, at 121, 122–23.

38. Hall, *supra* note 29, at 87 (citation omitted).

39. Theodore D. Fuller et al., *Chronic Stress and Psychological Well-Being: Evidence from Thailand on Household Crowding*, 42 SOC. SCI. & MED. 265, 267 (1996) (citation omitted). This view is echoed by Desmond Morris, who writes, "Each kind of animal has evolved to exist in a certain amount of living space. In both the animal zoo and the human zoo [when] this space is severely curtailed . . . the consequences can be serious." DESMOND MORRIS, THE HUMAN ZOO 39 (1969).

These results are supported by a number of more recent studies.[40] Overcrowding in prisons has been linked to violence,[41] depression,[42] suicide,[43] psychological disorders,[44] and recidivism.[45]

Given all of this, one can, with great confidence, claim that privacy is valuable for beings like us. The ability to regulate access to our bodies, capacities, and powers, as well as sensitive personal information, is an essential part of human flourishing and well-being.

II. TOWARD INFORMATIONAL PRIVACY RIGHTS

While it might be admitted that privacy, broadly defined as a right to control access to bodies and information, is morally valuable, it has not been established that individuals have moral claims to control personal information. One way to begin is by asking how claims to control intangible objects, like facts about someone, are generated. In the argument that follows, I will employ a version of John Locke's proviso on acquisition: "For this labor being the unquestionable property of the laborer, no man but he can have a right to what that is once joined to, at least where there is *enough and as good left . . . for others.*"[46] Locke claims that so long as the proviso that enough and as good is satisfied, an acquisition does not prejudice anyone. Viewed as a kind of "no harm, no foul" rule, actions that pass this standard leave little room for rational

---

40. *See* Andrew Baum & Stuart Koman, *Differential Response to Anticipated Crowding: Psychological Effects of Social and Spatial Density*, 34 J. PERSONALITY & SOC. PSYCHOL. 526, 535 (1976); David P. Farrington & Christopher P. Nuttall, *Prison Size, Overcrowding, Prison Violence, and Recidivism*, 8 J. CRIM. JUST. 221, 230 (1980); Fuller et al., *supra* note 39, at 277; Paul B. Paulus, Garvin McCain & Verne C. Cox, *Death Rates, Psychiatric Commitments, Blood Pressure, and Perceived Crowding as a Function of Institutional Crowding*, 3 ENVTL. PSYCHOL. & NONVERBAL BEHAV. 107, 114 (1978); R. Barry Ruback & Timothy S. Carr, *Crowding in a Woman's Prison: Attitudinal and Behavioral Effects*, 14 J. APPLIED SOC. PSYCHOL. 57, 66 (1984); *see also* Jes Clauson-Kaas et al., *Urban Health: Human Settlement Indicators of Crowding*, 18 THIRD WORLD PLAN. REV. 349, 353 (1996); Griscom Morgan, *Mental and Social Health and Population Density*, 20 J. HUM. REL. 196, 198 (1972). *But see* John N. Edwards & Alan Booth, *Crowding and Human Sexual Behavior*, 55 SOC. FORCES 791, 805 (1977) (finding that human sexual behavior is not appreciably influenced by crowded conditions).

41. Edwin I. Megargee, *The Association of Population Density, Reduced Space, and Uncomfortable Temperatures with Misconduct in a Prison Community*, 5 AM. J. COMMUNITY PSYCHOL. 289, 294 (1977); Frank J. Porporino & Kimberly Dudley, *An Analysis of the Effects of Overcrowding in Canadian Penitentiaries* 8–16 (Solicitor Gen. of Can., User Rep. No. 1984-06, 1984).

42. *See* sources cited *supra* note 40.

43. GARVIN MCCAIN, VERNE C. COX & PAUL B. PAULUS, U.S. DEP'T OF JUST., THE EFFECT OF PRISON CROWDING ON INMATE BEHAVIOR 113–15 (1980).

44. Paulus, McCain & Cox, *supra* note 40, at 112.

45. Farrington & Nuttall, *supra* note 40, at 229.

46. JOHN LOCKE, THE SECOND TREATISE OF GOVERNMENT 17 (Thomas Peardon ed., Bobbs-Merrill Co. 1952) (1690) (emphasis added).

complaint—I will call this version of Locke's proviso a "Pareto-based proviso."[47] Consider the following argument.

P1. The value of privacy related to human well-being grounds a weak presumptive claim to use and control personal information.
P2. Respect for persons, possessions, self-creation, and project pursuit grounds a weak presumptive claim to use and control personal information.
P3. If no one is worsened by such use, then the weak presumptive claims generated by the value of privacy and respect for persons are undefeated—actions that pass a Pareto-based proviso are permitted (no harm, no foul).
P4. It is typically the case that others are not worsened by some individual's use and possession of their own personal information.
C5. Thus, the weak presumptive claims to use and control such information are, in many cases, undefeated, and moral claims (perhaps rights) emerge.

The importance of privacy for human well-being, along with a concession that the promotion of certain fundamental values is a moral requirement, may provide adequate support for the first premise. Only a pure deontologist would deny that good and bad consequences, especially those related to basic needs, do not generate weak presumptive claims.

Support for the second premise builds on the notion of respect for persons as moral agents. Without justification, it would be wrong to take personal information and leave the original possessor without it—as it would be to wrest an apple from someone who just plucked it from an unowned tree. Developing one's capacities and intellectual effort and engaging in lifelong project pursuit are generally voluntary activities that

47. The "Pareto" condition is named after Vilfredo Pareto (1848–1923), an Italian economist and sociologist. The Pareto condition is defined as: One state of the world, S_1, is Pareto-superior to another, S_2, if and only if no one is worse off in S_1 than in S_2, and at least one person is better off in S_1 than in S_2. S_1 is *strongly* Pareto-superior to S_2 if everyone is better off in S_1 than in S_2, and *weakly* Pareto-superior if at least one person is better off and no one is worse off. State S_1 is Pareto-optimal if no state is Pareto-superior to S_1: it is *strongly* Pareto-optimal if no state is *weakly* Pareto-superior to it, and *weakly* Pareto-optimal if no state is *strongly* Pareto-superior to it. Throughout this paper I will use "Pareto" as a "super-weak" condition, namely to mean that no one is worsened. *See* G.A. Cohen, *The Pareto Argument for Inequality*, 12 SOC. PHIL. & POL'Y 160, 160–61 n.4 (1995).

can be unpleasant, exhilarating, and everything in between. That we voluntarily do these things as sovereign moral agents may be enough to warrant presumptive noninterference claims against others. In doing these things, we create the facts of our lives. Acknowledging weak presumptive claims to use and control personal information about these activities might be grounded in respect for persons and moral desert. Given that the first two premises establish the same point—they are redundant—if either is correct, then the argument goes forward.

A. Bettering, Worsening, and the Baseline Problem

Providing support for the third premise requires a clarification and defense of a Pareto-based proviso. In terms of clarification, we must adopt an account of value so that moral bettering and worsening can be determined. An individual could be worsened in terms of subjective preference, satisfaction, wealth, happiness, freedoms, opportunities, et cetera. Which of these count in determining bettering and worsening? Second, once the terms of being worsened have been resolved, what two situations are we going to compare to determine if someone has been worsened? Is the question one of how others are now, after my appropriation, compared to how they would have been were I absent, or if I had not appropriated, or some other state? Here we are trying to answer the question: "Worsened relevant to what?" This is known as the baseline problem.

In principle, the model of informational privacy being sketched is consistent with a wide range of value theories.[48] So long as the preferred value theory has the resources to determine bettering and worsening with reference to the use and control of personal information, then Pareto-superior moves can be made and justified.[49] For now, assume an Aristotelian eudaemonist account of value exhibited by the following theses is correct.

---

48. It has been argued that subjective preference satisfaction theories fail to give an adequate account of bettering and worsening. *See* Donald C. Hubin & Mark B. Lambeth, *Providing for Rights*, 27 DIALOGUE 489, 492 (1988); Adam D. Moore, *Values, Objectivity, and Relationalism*, 38 J. VALUE INQUIRY 75, 76–80 (2004).

49. Someone could object and claim that being permitted to use and control personal information because one satisfies a nonworsening requirement is not a *justification*. I may not morally worsen anyone by standing on my head at the bus stop—such actions are permitted but not justified. First, little would be lost by just dropping talk of justification in favor of what is permitted. Second, given that such actions, however silly, do not worsen and are within my rights, I would argue that they are justified—morality requires nothing more of me. *See* IMMANUEL KANT, FUNDAMENTAL PRINCIPLES OF THE METAPHYSIC OF MORALS 33 (Thomas K. Abbott trans., Bobbs-Merrill Co. 1st ed. 1949) (1785).

1. Human well-being or flourishing is the sole standard of intrinsic value.
2. Human persons are rational project pursuers, and well-being or flourishing is attained through the setting, pursuing, and completion of life goals and projects.[50]
3. The control of physical and intangible objects is valuable. At a specific time, each individual has a certain set of things she can freely use and other things she owns, but she also has certain opportunities to use and appropriate things. This complex set of opportunities, along with what she can now freely use or has rights over, constitutes her position materially—this set constitutes her level of material well-being.[51]

While it is certainly the case that there is more to bettering and worsening than an individual's level of material well-being, including opportunity costs, I will not pursue this matter further at present. Needless to say, a full-blown account of value will explicate all the ways in which individuals can be bettered and worsened with reference to acquisition. Moreover, as noted before, it is not crucial to the view being presented to defend some preferred theory of value against all comers. Whatever value theory is ultimately correct, if it has the ability to determine bettering and worsening with reference to the use and control of personal information, then a nonworsening standard can be used to determine when weak presumptive claims to use and control are undefeated.

Turning to the baseline problem (what two situations do we compare to determine moral bettering and worsening?), I believe that we should affirm the following base point. We compare how someone is after an action to the moment before. Consider a common case dealing with worsening: the face puncher case. When Crusoe punches Friday in the face we say that Friday has been worsened compared to the moment before the punch. We do not compare Friday's state of pain after the punching to his condition a month before when, let us suppose, he was in great pain due

50. For similar views see ARISTOTLE, NICOMACHEAN ETHICS, bk. I, X (Martin Ostwald trans., Bobbs-Merrill Co. 1962) (350 B.C.E.); KANT, *supra* note 49, at 42–45; LOREN E. LOMASKY, PERSONS, RIGHTS, AND THE MORAL COMMUNITY 26–27, 38 (1987); RALPH BARTON PERRY, GENERAL THEORY OF VALUE 181–82, 201–02 (Harvard Univ. Press 1950) (1926); JOHN RAWLS, A THEORY OF JUSTICE 408–09 (1971); HENRY SIDGWICK, THE METHODS OF ETHICS 46–49 (Hackett Publ'g Co. 1981) (1907).

51. The argument in support of the value of privacy offered earlier would support this view. *See supra* notes 26–45 and accompanying text.

to falling into a fire. Since an individual's level of material well-being changes over time, the baseline of comparison should also change.

As with the baseline which compares how someone is after an action to a month ago, the following baseline is also questionable. Suppose we compare how Friday is when he gets to use and control some value *V* to his condition where he does not get to use or control *V*. On this account, whenever anyone exclusively uses and controls *V*, they worsen others. Assuming that water is valuable, Crusoe worsens Friday when Crusoe takes a drink. Alas, Friday would be better if he got to drink the water in question *even if they are both standing by an endless stream of perfectly good drinking water*. Such baselines are indefensible because they produce overbroad accounts of moral bettering and worsening.[52]

A Pareto-based proviso indicates when others may have legitimate complaints against an established weak presumptive claim of use and possession. If in possessing and using their own personal information no one is worsened relative to the appropriate base point, then no one could have a compelling claim that would override the weak presumptive claims already in place. Put another way, an objection to appropriation, which is a unilateral changing of the moral landscape, would focus on the impact of the appropriation on others. But if this unilateral changing of the moral landscape makes no one worse off, there is little room for rational criticism.[53]

Several other points can be offered in support of a Pareto-based proviso as well. A "no harm, no foul" principle leaves moral room for individuals to live their lives as they see fit. While consequences matter, there is no maximization requirement—no required trade-offs of someone's lifelong goals and projects for mere incremental increases in social utility. In this way, a Pareto-based proviso accords with our considered convictions regarding respect for persons, and at the same time, accommodates consequentialist views linking theories of the good and theories of the right.

The truth of the fourth premise seems fairly obvious in light of my characterization of a Pareto-based proviso. When an individual uses and controls his own personal information, it will be the case that others are

---

52. For more about the difficulties in determining a baseline, see SHELLY KAGAN, THE LIMITS OF MORALITY 87–89 (1989); Hubin & Lambeth, *supra* note 48, at 492–93.

53. To adopt a less stringent principle would permit individuals, in bettering themselves, to worsen others. Such provisos on acquisition are troubling because they may open the door to predatory activity. To require individuals, in bettering themselves, to better others is to require them to give others free rides. Both of these standards are open to rational complaint. *See* ROBERT NOZICK, ANARCHY, STATE, AND UTOPIA 185–86 (1974) (discussing claims of justice in a hypothetical "Robinson Crusoe" case where ten stranded individuals have varying degrees of success fending for themselves).

not necessarily worsened. Consider some health-related fact that Crusoe comes to know about himself. To consider if Friday has been worsened, we compare how he is prior to Crusoe's coming to know the fact in question to Friday's situation after Crusoe's discovery. In either case, Friday is unaware and is not worsened by Crusoe's use and control. On the other hand, suppose that Crusoe knows that he is a violent sleepwalker and Friday is planning to sleep nearby. In this case, it seems that Friday has been—or will be—worsened by Crusoe's nondisclosure.

If the argument so far has been compelling, then it will be conceded that individuals have moral claims to use and control their own personal information. But since information is nonrivalrous, it is not clear that using and controlling personal information about others worsens them. To simplify matters, imagine a state of nature situation where Fred exists in isolation. Over the years, Fred may acquire a host of information about himself—say, for example, that he likes spicy food. In fact each of Fred's actions, his life story so to speak, may be captured as information. Suppose that when Ginger comes along, she is not worsened by Fred's possession and use of the aforementioned information. Thus, Fred's use and possession claims would be undefeated, and moral claims may emerge. Nevertheless, Fred's claims to control such information do not exclude the possibility of others owning or using such information.

In seeking to use and possess information about Fred, Ginger does not *necessarily* worsen Fred. Suppose that upon seeing him, Ginger notes that Fred has green eyes. Surely Ginger's mere possession of such information does not worsen Fred relative to how he would be had Ginger never come along or had the acquisition not occurred. But when Ginger offers information about Fred for public consumption—suppose that she shares this information with a much wider audience than Fred could have ever reached via daily public activity—she does worsen him in terms of increased risk, commercial exploitation, and the like.

B. The Risk Argument

Central to the risk argument is the claim that in connected societies where information trading is both efficient and nearly costless, disclosure of personal information opens individuals up to certain risks, for example, being controlled by entities with their own agendas.[54] Typically, such

54. Although not my direct concern here, I believe the risk argument could be modified to apply to small unconnected or nonwired communities as well.

control comes in two flavors. First, governments use such information to retain domination and expand power.[55] Second, corporations may use personal information to overwhelm individuals in a sea of solicitations and promotional advertisements or to control their employees. Sharing personal information about someone else with a third party—say a home address and religious affiliation—may have serious consequences. German Jews in the 1940s, and more recently American Muslims, know this all too well.

Two further examples should suffice in establishing the plausibility of this claim. Keeping records of citizens has been, and continues to be, a way for governments to maintain control over their populations. Nicholas Kristof writes:

> As part of China's complex system of social control and surveillance, the authorities keep a . . . file, on virtually everyone except peasants. Indeed, most Chinese have two [files]: one at their workplace and another in their local police station.
>
> . . . .
>
> A file is opened on each urban citizen when he or she enters elementary school, and it shadows the person throughout life, moving on to high school, college and employer. Particularly for officials, students, professors and Communist Party members, [these files] contain political evaluations that affect career prospects and permission to leave the country.[56]

A different case, but one that is equally alarming, is what happened in a small village in Greece. In Orchemenos, Greece, there are many individuals who have a gene that causes sickle-shaped red blood cells. The problem is that when two parents both carry the gene, their offspring may develop sickle-cell anemia. In an effort to prevent this disease, government researchers tested everyone in the village so that marriages between gene carriers could be avoided. In the end, the carriers became a shunned subclass forced to marry among themselves, making

---

55. The following quote from a Chinese military newspaper applies a number of these issues to information war:

> After the Gulf War, when everyone was looking forward to eternal peace, a new military revolution emerged. This revolution is essentially a transformation from the mechanized warfare of the industrial age to the information warfare of the information age. Information warfare is a war of decisions and control, a war of knowledge, and a war of intellect. The aim of information warfare will be gradually changed from 'preserving oneself and wiping out the enemy' to 'preserving oneself and controlling the opponent.' Information warfare includes electronic warfare, tactical deception, strategic deterrence, propaganda warfare, psychological warfare, network warfare, and structural sabotage.

John Carlin, *A Farewell to Arms*, WIRED, May 1997, at 51, 54 (quoting Jiefangjun Bao, Chinese Army newspaper).

56. Nicholas D. Kristof, *Beijing Journal: Where Each Worker is Yoked to a Personal File*, N.Y. TIMES, Mar. 16, 1992, at A4; *see also* ANNE WELLS BRANSCOMB, WHO OWNS INFORMATION? 16 (1994).

the situation even worse than before.[57] While the researcher's goals were noble, they obviously failed to foresee the ramifications of disclosing this kind of personal information.

In the typical case, without video, audio, and other kinds of robust surveillance, when Fred steps out on a public street he both creates certain facts about himself and relinquishes exclusive control of this information to those who share the public domain. The information captured by others is held in nonpermanent mediums like memory and is acquired by a relatively small number of people. In such cases, Fred incurs few risks, and the sharing of such information by second and third parties poses little threat. Please note that Fred could disguise himself or go out at night to further limit public access to personal information. Hinting at the property rights argument to come, Fred could use his property to justifiably limit access to personal information.

But when such information is captured digitally via video and audio surveillance or with some other more permanent medium, Fred is subjected to increased risks. Such information may go unused for decades and then be resurrected by those in power or with commercial agendas. In societies where personal information trading or data mining is facilitated through the use of technology, like digital environments, the use and control of personal information opens individuals up to risks and losses. If so, the disclosure of such information will worsen Fred relative to the base point, and a step toward informational privacy will have been established.

A serious objection to the risk argument is that maybe the risks imposed on individuals through the manipulation of personal information are counterbalanced by other values, such as increased opportunities or security. Data mining companies that gather information about Ginger's purchasing habits may be able to more narrowly pitch products and services. If Ginger likes cowboy boots, data mining companies could provide her with information about the most up-to-date styles. Alternatively, Ginger's government could provide enhanced security for her and others by using data mining techniques to search for criminal behavior.

As an admittedly imperfect analogy, consider the risks foisted on someone else when they are included in a game of Russian roulette without consenting. The typical game consists of a gun with six chambers, one

57. Charles Platt, *Evolution Revolution*, WIRED, Jan. 1997, at 158, 200.

bullet, and somebody's head. After loading the bullet and spinning the chamber, the gun is pointed at someone and the trigger is pulled. Surely the risks involved in such a game worsen the victim relative to the appropriate base point. Nevertheless, one could argue that having digitally stored personal information available for others to exploit is not like playing a game where the gun has only six chambers—it is more like a game where the gun has a thousand chambers and some of the chambers yield benefits, not burdens. True enough, but we are not playing a one-round game. Imagine playing an iterated game with hundreds, if not thousands, of rounds played over a lifetime. Moreover, as one plays the game, the risks of certain payoffs may increase with the changing times. And in the typical case, the burdens and benefits will be imposed, not freely chosen.

Two further considerations suggested by Helen Nissenbaum deserve mention at this point. Nissenbaum notes that data shifting—using information gathered for one purpose in some new way—violates what she calls contextual integrity. "In the public surveillance currently practiced, information is routinely shifted from one sphere to another, as when, for example, information about your supermarket purchases is sold to a list service for magazine subscriptions."[58] An admittedly extreme case of data shifting occurred when a stalker secured actress Rebecca Schaeffer's home address from certain state licensing records and murdered her.[59] Moreover, the digitization of information coupled with the expansion of computer networks has allowed information aggregation of a sort not seen before. Information that may be freely given in different contexts for various purposes is collected in digital profiles that are then sold. Data shifting and aggregation open up individuals to unforeseen and unconsented-to risks.

These considerations provide a compelling answer to what might be called the consent argument *against* informational privacy. On this view, individuals have no privacy rights because they have—by stepping into the public domain or by sharing information—agreed that others may own and control this information. But even if consent, however thin it may be, is given for the initial disclosure of disparate bits of information, it does not follow that consent has also been given for data shifting and aggregation of this information. The notion of consent implied in this argument against informational privacy may also be challenged. Appearing in public is a necessity for most of us.

---

58. Helen Nissenbaum, *Protecting Privacy in an Information Age: The Problem of Privacy in Public*, 17 LAW & PHIL. 584, 585 (1998).

59. Paul Jacobs, *Addresses at DMV Remain Accessible*, L.A. TIMES, Aug. 19, 1991, at A3.

This is not to say that privacy should never be overridden for the sake of increased security or market opportunities, but given the risks and benefits of such disclosure, the rule, both moral and legal, should be against allowing such activity.

C. The Bodily Access and Property Rights Argument

Suppose that Fred creates and wears an antidisclosure suit that shields him in public spaces entirely. All that his fellows know is that someone is present—they do not know if Fred is old or young, male or female, tall or short, et cetera. In simply wearing his antidisclosure suit Fred does nothing wrong—he does not necessarily worsen anyone. In this example, to discover information about Fred would require violating his property rights or liberty rights. Alas, the suit and what it shields is his to control. While odd and probably perverse, if Fred were to reveal nothing about himself to anyone at any time, it would be perfectly appropriate.[60] Another way to put the point is that Fred's rights to control access to his body, capacities, and powers—what might be called physical privacy rights—coupled with property rights will afford him near complete control over the information that he creates through daily activity.

As noted earlier, the information that Fred chooses to reveal about himself may be owned by Ginger and others. Part of reaching out and developing social relationships with others will be the voluntary disclosure of personal information. But whatever kind of information we are considering, there is a gathering point that individuals have control over. For example, in purchasing a new car and filling out the car loan application, no one would deny 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. In agreeing with this view, one first has to agree that individuals have the right to control their own personal information—that is, binding agreements about controlling information presuppose that one of the parties has a moral claim to control this information. This is just another way of affirming the argument offered in support of individual claims to control personal information.

60. Assuming of course that Fred is not shielding immoral *and* criminal activity.

Aside from controlling information gathering points, there is at least one other way in which individuals can protect themselves from invasions of privacy due to digital monitoring.[61] J.P. Barlow of the Electronic Frontier Foundation was the first to suggest this idea. It may be possible to detach one's physical self from one's virtual self through the use of encryption—the online equivalent of an antimonitoring suit. The idea is to encrypt all information that links data about you to your name, address, or social security number—leaving no unencrypted links between your physical self and your electronic identity. Individuals would then just become a number identified with data in the form of e-mail letters, purchasing habits, voting records, credit reports, medical records, and the like.[62]

To summarize the bodily control and property rights argument in support of informational privacy, we begin with four plausible propositions. First, individuals have use and possession claims concerning information about themselves. Second, individuals have access control rights over their bodies, capacities, and powers. Third, individuals may acquire physical and intellectual property that will aid in restricting access to personal information. And finally, individuals have a general moral and legal right to make contracts. Taken together, these rights, claims, and liberties provide the foundation for informational privacy.

One problem for this second argument in support of informational privacy is that given disparities in holdings and the subsequent ability to fence oneself off from the outside world, some individuals will have more privacy than others. The rich will be able to hide behind walls, fences, lawyers, and butlers, while the not so fortunate will be left exposed to public consumption. Consider the following case.

> [O]n the night of October 30, 1979 . . . an NBC television camera crew entered the apartment of Dave and Brownie Miller in Los Angeles, without their consent, to film the activities of Los Angeles Fire Department paramedics called to the Miller home to administer life-saving techniques to Dave Miller, who had suffered a heart attack in his bedroom. The NBC television camera crew not only filmed the paramedics' attempts to assist Miller, but NBC used the film on its nightly news without obtaining anyone's consent. In addition, after it had received complaints from both Brownie Miller and her daughter, Marlene Miller Belloni, NBC later used portions of the film in a commercial advertising an NBC "mini-documentary" about the paramedics' work.[63]

---

61. For numerous other ways to maximize one's control over personal information, see DEBORAH G. JOHNSON, COMPUTERS ETHICS 134–35 (3d ed. 2001) (quoting Gary T. Marx, *Privacy & Technology*, WHOLE EARTH REV., Winter 1991, at 90, 94).

62. For more about how technology can protect privacy and security, see Ann Cavoukian, *Security Technologies Enabling Privacy (STEPs): Time for a Paradigm Shift* (Off. Info. & Privacy Commissioner Ont., Toronto, Ont.), June 1, 2002, at 7–9, *available at* http://www.ipc.on.ca/images/resources/steps.pdf.

63. Miller v. NBC, 232 Cal. Rptr. 668, 670 (Cal. Ct. App. 1986).

One would suspect that if the Millers had employed guards, security fences, and perhaps "high priced" lawyers, they would have successfully protected their privacy.

While true, I believe that this sort of objection is fairly anemic. Individuals will still be able to keep sensitive personal information secret by manipulating what property they do hold. It is not as if wearing disguises or paying cash will cease to work. Individuals with little in terms of property holdings will still be able to restrict information leakage through second and third parties via contracts and agreements. And finally, if moral norms are to be reflected in the law, legal privacy guarantees codified in state and federal statutes will cover everyone.

III. APPLICATIONS AND ILLUSTRATIONS

Having said all of this, I would like to test the model of informational privacy that has been offered by examining two cases dealing with personal information control. A canonical example of a privacy violation is all too familiar in garden-variety peeping Tom cases. A second case, one that will be examined in some detail, concerns privacy and governmental surveillance.

A. Peeping Toms and Informational Privacy

Suppose Tom, after sneaking through the bushes and pulling aside a blind, licentiously watches Ginger who is in her house. Maybe Tom watches Ginger take a shower or dress for bed. We can all agree that what Tom is doing is immoral—and illegal—given that Ginger does not know and has not consented to being watched. But why? The typical answer is that Tom violated Ginger's right to privacy.

In a two-person world, it might be difficult to see how Ginger is worsened by Tom's peeping. Putting aside property rights violations—Tom is standing on Ginger's land and has interfered with Ginger's control of the window blind—it would seem that Ginger is not worsened in any objective sense. Tom's actions do not open Ginger up to third party risks of control or manipulation, because there are no third parties. Moreover, suppose that he is not recording the encounter. Any information obtained will fade with his memory.

It does no good to say that Tom's peeping worsens Ginger because she has a general wish or desire not to be watched. Mere desires and wishes are not the foundations of value claims; however, they may reflect such

claims.[64] In such a contrived two-person world, we may have to say that Tom does nothing wrong in watching Ginger. In the real world, however, Tom's acquisition of information about Ginger does create risks that are morally relevant to Ginger's well-being. Maybe Tom innocently mentions Ginger's open window to James the burglar. Moreover, Ginger's knowledge of Tom's act is irrelevant to questions of bettering and worsening. She might never know of the risks foisted on her by Tom, yet still be worsened.

As we move upward from the two-person case to institutions, legal systems, and cultural norms that affect relations across numerous individuals, and if we keep in mind that privacy is a basic need, then we will have provided adequate grounds for forbidding Tom's behavior. His act by itself may not worsen, but allowing such a practice would.

B. Privacy, Secrecy, and Government Surveillance

In times of national crisis, citizens are often asked to trade liberty and privacy for security. And why not, it is argued, if we can obtain a fair amount of security for just a little privacy? Moreover, the surveillance that enhances security need not be overly intrusive or life-altering. It is not as if government agents need to physically search each and every suspect or those linked to a suspect. Advancements in digital technology have made such surveillance relatively unobtrusive. Video monitoring, global positioning systems, biometric technologies, along with data surveillance may provide law enforcement officials monitoring tools without also unduly burdening those being watched.

Against this view are those who maintain that we should be worried about trading privacy for security. Criminals and terrorists, it is argued, are nowhere near as dangerous as governments. There are far too many examples for us to deny Lord Acton's dictum, "Power tends to corrupt, and absolute power corrupts absolutely."[65] If information control yields power, and total information awareness radically expands that power, then we have good reason to pause before trading privacy for security.

If the model of informational privacy that has been presented is correct, then individuals have moral claims to control personal information. Due to space considerations, I will not provide arguments justifying physical privacy claims[66] or security rights—please assume that individuals

---

64. For a defense of "objectivity" in relation to value claims and an attack on "subjective" accounts of moral value, see Moore, *supra* note 48, at 80–82.

65. Letter from Lord Acton to Bishop Mandell Creighton (Apr. 3, 1887), *in* 1 LIFE AND LETTERS OF MANDELL CREIGHTON 372 (1904).

66. This argument runs parallel to the argument for information privacy already considered. The primary difference is that use of one's body, capacities, and powers is

have rights to control access to their bodies and specific locations, and that individuals have security rights (perhaps this right is simply a combination of individual rights to life, property, and self-defense).[67] Given that security interests and privacy claims often conflict, what is needed is a generally agreed upon process for determining an appropriate balance. In this final part, I will consider the often-used "balancing test" view. Several cases will be presented which indicate how easily balancing arguments go awry. We should not blithely trust government officials with good intentions. I will argue that one way to appropriately balance privacy and security is (1) to insist upon establishing probable cause for an intrusion, (2) allow for robust judicial discretion on issuing warrants, and (3) ensure public oversight of the process and the reasoning involved.

---

rivalrous—unlike the use of information about others. Using or attempting to use someone else's body will, in the vast majority of cases, worsen them relative to the appropriate base point.

67. At first glance, security is valuable and can be separated into three distinct yet interconnected domains. At the most basic level, security affords individuals control over their lives, projects, and property. To be secure at this level is to have sovereignty over a private domain—it is to be free from unjustified interference from other individuals, corporations, and governments. At this level, privacy and security come bundled together.

At the second level, security protects groups, businesses, and corporations from unjustified interference with projects and property. Corporations need to be secure from industrial espionage, theft, and the like. Without this kind of control, businesses and corporations could not operate in a free market—not for long anyway. In any case, if we ask the question, "Why do we care about corporations and free markets?," we are quickly led back to security at the individual level. We value security at the level of groups, businesses, and corporations because these entities are intertwined with security at the personal level. It is through these groups that many of us pursue lifelong plans and projects and order our lives as we see fit. Few would maintain that these groups are valuable independent of their impact on individual lives. Privacy and security come bundled together at this level as well, although in a different way. Through the use of walls, guards, and fences, groups are able to secure a private domain that may be necessary for the continued existence of groups and group activities.

There is also national security to consider. Here we are worried about the continued existence of a political union. Our institutions and markets need to be protected from foreign invasion, plagues, and terrorism. But again it seems that we value national security, not because some specific political union is valuable in itself, but because it is a necessary part of protecting individual liberty. Armed services, intelligence agencies, police departments, public health institutions, and legal systems provide security for groups, businesses, and at the most fundamental level, individuals.

C. A Brief Overview of Surveillance Law in the United States

Within the United States legal system, there are four ways that law enforcement agents can engage in surveillance.[68] First, there are warrants authorizing the interception of communications. Second, there are warrants authorizing the search of physical premises. For example, Title III of the Omnibus Crime Control and Safe Streets Act requires that law enforcement officials obtain a warrant from a judge to conduct surveillance in criminal cases.[69] To issue the warrant, the judge must find probable cause to believe that the suspect "is committing, has committed, or is about to commit a particular offense."[70] Third, there are provisions that allow trap-and-trace devices and pen traps. For example, trap-and-trace devices allow law enforcement agents to trace outgoing and incoming telephone numbers. Finally, there are subpoenas requiring the production of goods such as telephone logs or e-mail records. Unlike the first two methods of surveillance, the last two require a lower standard of justification. Trap-and-trace devices only require a sworn declaration that the information being sought is relevant to an investigation.[71] Court orders for records require that agents show that the information being sought is relevant and material to an ongoing investigation.[72] Moreover, each of these requirements applies only to domestic surveillance—monitoring individuals who are not American citizens is another matter.

Surveillance of American citizens is carried out by several agencies including city, county, and state police departments and the Federal Bureau of Investigation (FBI). The National Security Administration (NSA) and the Central Intelligence Agency (CIA) are forbidden by law from monitoring domestic activities and are responsible for conducting surveillance outside the United States.[73]

To clarify the intelligence gathering abilities of the FBI, CIA, and NSA, Congress enacted the Foreign Intelligence Act of 1978 (FISA).[74] Judicial oversight of FISA warrants was given to a newly created court

68. Jacob R. Lilly, *National Security at What Price?: A Look into Liberty Concerns in the Information Age Under the USA PATRIOT Act of 2001 and a Proposed Constitutional Test for Future Legislation*, 12 CORNELL J.L. & PUB. POL'Y 447, 457 (2003).

69. 18 U.S.C. § 2518(1) (2000); *see also* Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, 82 Stat. 197, 218.

70. 18 U.S.C. § 2518(3)(a) (2000).

71. 18 U.S.C. § 3122 (2000).

72. *See* 17 U.S.C. § 512(h)(2)(C) (2000).

73. *See* Exec. Order No. 12,333, 3 C.F.R. 200 (1982), *reprinted as amended in* 50 U.S.C. § 401 (2000).

74. Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, 92 Stat. 1783.

called the Foreign Intelligence Surveillance Court (FISC).[75] To obtain a FISC order allowing surveillance of a U.S. citizen, the government must show that the target is a foreign power or is the agent of a foreign power.[76] Since the information is not related to a criminal investigation, there is no requirement of probable cause—that is, government agents do not need to show that the target is, has, or will commit a crime. If the target is not a U.S. citizen, then no court order is necessary and only authorization from the Attorney General is required.[77]

The USA PATRIOT Act made numerous changes to the surveillance methods already mentioned. Below is a list of some of the changes. The PATRIOT Act:

1. Expands the government's ability to conduct covert "sneak and peak" searches. Government agents may take photographs, seize property, and not notify the target until a later time.[78]
2. Allows the inclusion of DNA information into databases of individuals convicted of "any crime of violence."[79]
3. Increases government surveillance abilities of suspected computer trespassers—any target suspected of violating the Computer Fraud and Abuse Act may be monitored without a court order.[80]
4. Increases the government's ability to access records held by third parties.[81] By expanding the use of FISA, targets "whose records are sought need not be an agent of a foreign power. United States citizens could be . . . investigated on account of activities connecting them to an investigation of international

---

75. FISA essentially allows electronic surveillance and physical searches of foreigners and U.S. citizens when there is "probable cause to believe that . . . the target . . . is a foreign power or an agent of a foreign power." Still, standards for obtaining a warrant are much less rigorous than under Title III . . . . Laurie Thomas Lee, *The USA PATRIOT Act and Telecommunications: Privacy Under Attack*, 29 RUTGERS COMPUTER & TECH. L.J. 371, 374–75 (2003) (citing 50 U.S.C. §§ 1804(a), 1805(a)(3)(A), 1823(a), 1824(a)(3)(A) (2000)).

76. *Id.*

77. 50 U.S.C. § 1802(a)(1) (2000).

78. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001, Pub. L. No. 107-56, § 213, 115 Stat. 272, 285–86 [hereinafter USA PATRIOT Act].

79. *Id.* § 503, 115 Stat. at 364.

80. *Id.* § 217, 115 Stat. at 290–91.

81. *Id.* § 215, 115 Stat. at 287.

terrorism."[82] In addition, FISC judges must issue a warrant if the application meets the requirements of Section 215.

Beyond the government surveillance powers already noted, the U.S. Constitution grants the President broad powers in times of crisis and war—in early 2002 President George W. Bush implemented a secret program that allowed the NSA to conduct warrantless searches of U.S. citizens. This program authorized the NSA to search international phone calls from U.S. citizens, thus sidestepping FISA.[83]

D. "Just Trust Us"—Trading Civil Rights for Security

A common view is that we should give the benefit of the doubt to those in power and assume that officials will not violate individual rights without just cause. Public officials typically seek office to promote the public good and are generally well meaning and sincere people—we should trust them to do what is right and fair.

Arguably, there are good reasons to distrust this method of establishing an appropriate balance between privacy and security. Justice Brandeis, dissenting in *Olmstead v. United States*, wrote:

> Experience should teach us to be most on our guard to protect liberty when the government's purposes are beneficent. Men born to freedom are naturally alert to repel invasion of their liberty by evil-minded rulers. The greatest dangers to liberty lurk in insidious encroachment by men of zeal, well-meaning but without understanding.[84]

Noting a few examples should suffice in demonstrating the perils of letting those in power set the guidelines for surveillance: Abraham Lincoln's suspension of the writ of habeas corpus in the border states;[85] Japanese-American internment during World War II;[86] McCarthy and the House Un-American Activities Committee;[87] *Laird v. Tatum*,[88] allowing

---

82. Lee, *supra* note 75, at 379.

83. James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. TIMES, Dec. 16, 2005, at A1.

84. 277 U.S. 438 (1928) (Brandeis, J., dissenting).

85. Lilly, *supra* note 68, at 450–51. Lilly notes that these civil rights violations were not the first in American history. "The Alien and Sedition Acts, Andrew Jackson's unlawful detention of reporter Louis Louailler, and military actions during 'Dorr's Rebellion' in 1842 all violated personal civil liberties in the name of national security." *Id.* at 450 n.14. "Habeas corpus" is Latin for "that you have the body." BLACK'S LAW DICTIONARY 728 (8th ed. 2004). *See also* U.S. CONST. amend. VI.

86. *See* Korematsu v. United States, 323 U.S. 214, 215–16, 223–24 (1944); Yasui v. United States, 320 U.S. 115, 116–17 (1943); Hirabayashi v. United States, 627 F. Supp. 1445, 1447 (W.D. Wash. 1986), *aff'd in part and rev'd in part*, 828 F.2d 591, 592–93 (9th Cir. 1987); Korematsu v. United States, 584 F. Supp. 1406, 1409 (N.D. Cal. 1984).

87. Lilly, *supra* note 68, at 453–54.

military surveillance of civilian activity;[89] and COINTELPRO, the FBI's covert action program against American citizens.[90] One of the more humorous examples comes from P.J. O'Rourke.

> The [United States Department of Agriculture] has over 106,000 employees . . . [and] they're too busy doing things like administering the Federal Wool and Mohair Program. According to the U.S General Accounting Office report to Congress on the 1990 farm bill, "The government established a wool and mohair price-support program in 1954 . . . to encourage domestic wool production *in the interest of national security*." Really, it says that. . . . From 1955 to 1980, $1.1 billion was spent on wool and mohair price supports, with 80 percent of that money going to a mere six thousand shepherds and (I guess) moherds. This is $146,400 per Bo Peep.[91]

A more current example comes from abuses related to the USA PATRIOT Act and the terrorist attacks of 9/11.[92] Here I am thinking of Al-Hussayen's detainment for more than a year for "providing expert advice and assistance" to terrorist organizations.[93] Finally, in March 2007, numerous

---

88. 408 U.S. 1, 13–14 (1972) (holding that plaintiffs did not have standing to challenge the Army's surveillance of civilian political activity).

89. *See* Laura W. Murphy, Director, ACLU Washington National Office, ACLU Looks at Domestic Surveillance and the Need to Watch the Watchers in Times of Crisis (Oct. 10, 2001), http://www.aclu.org/FreeSpeech/FreeSpeech.cfm?ID=9790&c=86.

90. S. REP. NO. 94-755, at 3–4 (1976).

91. P.J. O'ROURKE, PARLIAMENT OF WHORES: A LONE HUMORIST ATTEMPTS TO EXPLAIN THE ENTIRE U.S. GOVERNMENT 144–45 (1991) (emphasis added).

92. Consider how "terrorism" is now defined:

> A person engages in domestic terrorism if they do an act "dangerous to human life" that is a violation of the criminal laws of a state or the United States, if the act appears to be intended to: (i) intimidate or coerce a civilian population; (ii) influence the policy of a government by intimidation or coercion; or (iii) to affect the conduct of a government by mass destruction, assassination or kidnapping.

ACLU, How the USA PATRIOT Act Redefines "Domestic Terrorism" (Dec. 6, 2002), http://www.aclu.org/natsec/emergpowers/14444leg20021206.html (citing USA PATRIOT Act, *supra* note 78, § 802). If establishing (i)–(iii) is a matter of determining intentions, then the current debate over the legitimacy of torture may be seen in a new light. Alas, one way to determine the intentional status of a suspect is to torture him.

93. The Department of Justice also used the material support provisions of the Patriot Act to prosecute Muslim student Sami al-Hussayen for engaging in First Amendment activities. Section 805 of the Patriot Act made it a crime to provide material support in the form of "expert advice and assistance" to a designated foreign terrorist organization. Al-Hussayen, a 34-year old doctoral candidate at the University of Idaho and a computer expert, was charged with providing "expert advice and assistance" because, among other things, he volunteered as a Webmaster for the Islamic Assembly of North America—an organization the government had not put on its list of foreign terrorist

news agencies reported that the FBI had overstepped its authority and tried to cover it up. The audit by the Justice Department also found that

> the FBI had hatched an agreement with telephone companies allowing the agency to ask for information on more than 3,000 phone numbers—often without a subpoena, without an emergency or even without an investigative case. In 2006, the FBI then issued blanket letters authorizing many of the requests retroactively, according to agency officials and congressional aides briefed on the effort.[94]

"Just trust us" sentiments might have more force if robust accountability provisions accompanied them. But FISA courts meet in secret, their findings are almost never published, and only government officials appear before the court.[95] Bush's program authorizing the NSA to monitor international phone calls of U.S. citizens was secret—even more alarming to some, information about the program was withheld for a year by a "free press."[96] One can only wonder what other secret programs are currently in place.[97]

---

organizations. The government charged that this volunteer activity constituted expert advice and assistance.

Al-Hussayen's web pages provided many links, including links to "fatwas" that advocated criminal activity and suicide operations, but that were not written by al-Hussayen. Essentially, he was reporting what others said—something journalists do every day. Al-Hussayen's lawyer also established that Reuven Paz, a prosecution witness, admitted that he had posted much of the same information on his own website and that the BBC did as well. The Justice Department did not stop this abuse of the Patriot Act, and detained al-Hussayen for one and one-half years on minor immigration charges. It was a jury that stopped this abuse by finding al-Hussayen not guilty of all terrorism charges leveled against him. He was later deported on immigration charges.

Anthony D. Romero, ACLU Letter to Senator Feinstein Addressing the Abuses of the Patriot Act by the Government (Apr. 4, 2005), http://www.aclu.org/safefree/general/17563leg20050404.html (citation omitted).

94. Dan Eggen & John Solomen, *FBI Audit Prompts Calls for Reform; Some Lawmakers Suggest Limits on Patriot Act*, WASH. POST, Mar. 10, 2007, at A1.

95. The eagerness of many in law enforcement to dispense with the requirements of the Fourth Amendment was revealed in August 2002 by the secret court that oversees domestic intelligence spying (the "FISA Court"). Making public one of its opinions for the first time in history, the court revealed that it had rejected an attempt by the Bush Administration to allow criminal prosecutors to use intelligence warrants to evade the Fourth Amendment entirely. The court also noted that agents applying for warrants had regularly filed false and misleading information. That opinion is now on appeal.

ACLU, Surveillance Under the USA PATRIOT Act (Apr. 3, 2003), http://www.aclu.org/SafeandFree/SafeandFree.cfm?ID=12263&c=206.

96. *See* Eggen & Solomen, *supra* note 94. One theory about why President Bush would sidestep FISA, which has never rejected a warrant application, is that the information used as the basis of the search was obtained by U.S. operatives torturing prisoners outside the United States.

97. "Every thing secret degenerates, even the administration of justice; nothing is safe that does not show how it can bear discussion and publicity." Lord Acton, letter 74, (Jan. 23, 1861), *in* LORD ACTON AND HIS CIRCLE 165, 166 (Abbot Gasquet ed., Longmans, Green & Co. 1906).

Moreover, a generally recognized principle embedded in our Constitution is due process—individual rights are not to be violated or overridden without due process of law.[98] Secret courts and search programs that include no accountability provisions may violate due process.[99]

E. The Nothing to Hide Argument[100]

A counterpart to the "just trust us" argument is the nothing to hide argument. According to this argument, we are to balance the disvalue of privacy intrusions related to data mining and the like with the security interests of detecting and preventing terrorist attacks. I suppose we could weaken this further by merely referencing security interests, which would include but not be limited to terrorist attacks. A formal version of the argument might go something like this:

P1. When two fundamental interests conflict, we should adopt a balancing strategy, determine which interest is more compelling, and then sacrifice the lesser interest for the greater interest. If it is generally true that one sort of interest is more fundamental than another, we are warranted in adopting specific policies that seek to trade the lesser interest for the greater interest.

P2. In the conflict between privacy and security, it is almost always the case that security interests outweigh privacy interests. The privacy intrusions related to data mining or NSA surveillance are not as weighty as our security interests in stopping terrorism, et cetera—these sorts of privacy intrusions are more of a nuisance than a harm.

C3. So it follows that we should sacrifice privacy in these cases and perhaps adopt policies that allow privacy intrusions for security reasons.

One could easily attack premise 2—there are numerous harms associated with allowing surveillance that are conveniently minimized or forgotten by the "nothing to hide" crowd. The chilling effects on behavior, data aggregation, exclusion, and secondary use each ratchet up the harms

98. U.S. CONST. amend. XIV, § 1.

99. Secret courts and search programs may also violate "equal protection" guarantees when specific groups are targeted.

100. For a more rigorous analysis of this argument see Daniel J. Solove, *"I've Got Nothing to Hide" and Other Misunderstandings of Privacy*, 44 SAN DIEGO L. REV. 745 (2007).

caused by data monitoring and government surveillance. Daniel J. Solove notes, "[P]rivacy is threatened not by singular egregious acts, but by a slow series of relatively minor acts which gradually begin to add up."[101] Solove also points out, as I have already highlighted, that giving governments too much power undermines the mission of providing for security—the government itself becomes the threat to security.[102] John Locke put the point nicely: "This is to think that men are so foolish that they take care to avoid what mischiefs may be done them by *pole-Cats* or *foxes*, but are content, nay, think it safety, to be devoured by *lions*."[103] It is also important to note the risk of mischief associated with criminals and terrorists compared to the kinds of mischief perpetrated by governments—even our government. In cases where there is a lack of accountability provisions and independent oversight, governments may pose the greater security risk.

Consider a slight variation of the "nothing to hide" argument related to what I have called physical privacy. Suppose there was a way to complete body cavity searches without harming the target or being more than a mere nuisance. Perhaps we search the target after he has passed out drunk. Would anyone find it plausible to maintain a "nothing to hide" view in this case? I think not. And the reason might be that we are more confident in upholding these rights and the policies that protect these rights than we are of almost any cost-benefit analysis related to security. Whether rights are viewed as strategic rules that guide us to the best consequences, as Mill would argue, or understood as deontic-based constraints on consequentialist sorts of reasoning, we are more confident in them than in almost any "social good" calculation.[104] I am not saying that rights are absolute; they are just presumptively weighty. This line of argument is an attack on the first premise of the "nothing to hide" position offered above. In essence, it is the view that rights are resistant to cost-benefit or consequentialist sorts of arguments. Here we are rejecting the view that privacy interests are the sorts of things that can be traded for security.

Another worry for the "nothing to hide" argument has to do with justice and the distribution of harms. Jeremy Waldron writes:

> If security-gains for most people are being balanced against liberty-losses for a few, then we need to pay attention to the few/most dimension of the balance, not just the liberty/security dimension.

---

101. *Id.* at 769.
102. *Id.* at 766–67; *see also supra* notes 84–99 and accompanying text.
103. LOCKE, *supra* note 46, at 53.
104. JOHN STUART MILL, UTILITARIANISM 41–63 (George Sher ed., Hackett Publ'g Co. 1979) (1861); J.J.C. Smart, *Extreme and Restricted Utilitarianism*, 6 PHIL. Q. 344, 344–45 (1956). *See generally* DAVID LYONS, FORMS AND LIMITS OF UTILITARIANISM (1965) (comparing various utilitarian theories).

. . . .

> . . . We are not balancing the rights of the innocent against the rights of the guilty. We are balancing the interests in life or liberty of the one innocent man against the security interests of those of the rest of us . . . that will be served if [criminals] are convicted by the procedures that lead to the wrongful conviction of the innocent.[105]

The distribution aspect is highlighted when surveillance policies pick targets based on appearance, ethnicity, or religion. If the burden of surveillance policy and the corresponding harms fall on one portion of society, we may have a problem of justice.

Waldron also notes that balancers who seek to trade privacy for security typically have little evidence of the overall effect of some surveillance policy, and whether there might be some other policy that better protects both privacy and security.[106] Consider just for example, almost any predominately developed "isolationist" country—perhaps Switzerland. Although admittedly I have not researched this claim, my guess is that these sorts of countries do not have much terrorist activity and likely do not have higher crime rates than the United States. The point here is that one way to obtain more security would be to change our selectively interventionist policies. In this way security and privacy could be protected.

F. The "Security Trumps" View

According to what might be called the "security trumps" view,[107] whenever privacy and security conflict, security wins—that is, security

---

105. Jeremy Waldron, *Security and Liberty: The Image of Balance*, 11 J. POL. PHIL. 191, 203–04 (2003).

106. *Id.* at 208–09.

107. Balancing arguments that seek to justify trading privacy for security are typically based on the assumption that privacy and security are measurable values that can be compared and traded like diamonds for gold. This view does not need to hold that we can trade six units of privacy for ten units of security. All we need to be able to do is justifiably claim that there is some amount of privacy that we would be willing to trade for some other amount of security.

But it is not at all clear how these trade-offs should work or how these items should be measured. For example, we may agree that there is no amount of ice cream that we would trade for our arms and legs. This case is based on Laurence H. Tribe, *Policy Science: Analysis or Ideology?*, 2 PHIL. & PUB. AFF. 66, 90 (1972). *See also* James Griffin, *Are there Incommensurable Values?*, 7 PHIL. & PUB. AFF. 44 (1977). Ice cream may be tasty, but it is not on the same scale as arms and legs. Or suppose we were faced with the choice of living normally for a year and then dying or having a brain operation and living in a vegetative state for thirty years. *See* Griffin, *supra*, at 47. It is not at all clear that any amount of "vegetative" existence is worth one year of normal living.

is more fundamental and valuable than privacy. First, without arguments, it is not clear why a "security trumps" view should be adopted over a "privacy trumps" view. Privacy or perhaps self-ownership seems at least as fundamental or intuitively weighty as security.

Foreshadowing things to come, it is not at all clear—at least in some cases—that privacy does not enhance security and vice versa. Suppose that rights afforded their holders specific sorts of powers. For example, Fred's privacy rights generate in him a god-like power to completely control access to his body and to information about him. If we had such powers, we would also have increased security. Furthermore, if we had complete security in our bodies and property, including informational security, we would have secured privacy as well. The tension between privacy and security arises because these values cannot be protected by individuals acting alone. Nevertheless, it is important to note that as these services are contracted out to other agents, like governments, we grant these parties power over us—power that may undermine security and privacy.

Continuing with the "security trumps" argument, it would seem odd to maintain that any increase in security should be preferred to any increase in privacy or any decrease in privacy is to be preferred to any decrease in security. Such a view would sanction massive violations of privacy for mere incremental and perhaps momentary gains in security. Also, given that others will provide security and power is likely a necessary part of providing security, we have strong prudential reasons to reject the "security trumps" view. If those who provide security were saints, then perhaps there would be little to worry about. The cases already presented are sufficient to show that we are not dealing with saints.

G. Turning Security Arguments on Their Heads

It is false to claim that in every case more privacy means less security or that more security entails less privacy. Security arguments actually

---

James Griffin is not so sure arguing that if dessert consumption was not subject to diminishing marginal utility (roughly meaning the more you have of something the less valuable it is), was worth something, and we could contemplate the large numbers involved, there may be a trade-off point. *Id.* at 44. In addition, living a long life in a vegetative state may have no value so the second case has no force—there are no values to trade-off in this case.

I think that it is clear that most of us would trade privacy for a certain level of monetary compensation. Suppose someone offered you a cool million dollars to watch you for a day. Nevertheless, coming up with an ordinal, cardinal, or mere better than/less than ranking of some amount of privacy compared to some amount of security would be difficult, especially when such calculations are related to rules or legislation. For a discussion of incommensurability, see generally INCOMMENSURABILITY, INCOMPARABILITY, AND PRACTICAL REASON (Ruth Chang ed., 1997).

cut the other direction in some cases. For example, it is only through enhanced privacy protections that we can obtain appropriate levels of security against industrial espionage, unwarranted invasions into private domains, and information warfare or terrorism.

An example of how privacy protections enhance security comes from the debate over encryption standards for electronic communications and computer networks. Although the NSA's position is that the widespread use of encryption software will allow criminals a sanctuary to exchange information necessary for the completion of illegal activities, consider how easily this security argument can be turned on its head. National security for government agencies, companies, and individuals actually *requires* strong encryption. Spies have admitted to "tapping in" and collecting valuable information on U.S. companies—information that was then used to gain a competitive advantage.[108] A report from the Center for Strategic and International Studies Task Force on Information Warfare and Security notes, "Cyber terrorists could potentially overload telephone lines; disrupt air traffic control . . . scramble the software used by major financial institutions, hospitals, and other emergency services; . . . or sabotage the New York Stock Exchange."[109] Related to information war, it would seem that national security requires strong encryption, multilevel firewalls, and automated detection of attacks.

H. Balancing Privacy, Security, and Accountability

Suppose that there was good evidence that an attack was about to happen in a private domain. In this case we may be more confident that security interests outweigh privacy interests and allow the intrusion. To avoid the travesties already mentioned, we need a set of policies or rules that adequately protect privacy and security.[110]

---

108. JONATHAN WALLACE & MARK MANGAN, SEX, LAWS, AND CYBERSPACE 51 (1997).

109. Christopher Jones, *Averting an Electronic Waterloo*, WIRED, Dec. 16, 1998, http://www.wired.com/politics/law/news/1998/12/16875; *see also* Eric Talbot Jensen, *Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defense*, 38 STAN. J. INT'L L. 207, 207–08 (2002).

110. In *Olmstead v. United States*, 277 U.S. 438, 466 (1928), the court ruled that the Fourth Amendment against unreasonable searches and seizures applied to physical things like houses, notebooks, and receipts, but not to electronic communications. Thirty-nine years later the Supreme Court, in *Katz v. United States*, 389 U.S. 347 (1967), overturned the *Olmstead* decision, holding that privacy interests may be found in personal communications as well as "persons, houses, papers, and effects." *Id.* at 353 (quoting U.S. CONST. amend. IV). *Olmstead* and *Katz* represent the very issue we are considering—

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 concerns may be addressed with minimal impact on individual privacy. The requirement of probable cause puts the burden of proof in the appropriate place—invasions of private domains must be justified. The official seeking the warrant would highlight the security risks 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. In any event, the question of when security should override privacy would not be left to the subjective judgment of one individual or a small group of individuals with similar interests. Finally, sunlight provisions provide public oversight of the entire process, including the reasons for the warrant and the judicial ruling. In this way, public accountability is ensured at each step. Consider the following table that measures privacy interests across several dimensions.[111]

Magnitude of Invasion Duration, Extent, Means	
Slight	**Profound**
A one-time wire-tap of a cell phone conversation.	Total surveillance including data mining, electronic communications, physical movements.
Context	
Little Expectation	**Reasonable Expectation**
The subject will be monitored in "public"—perhaps as they walk down the street.	The subject will be monitored at their primary residence.
Consent	
Consented to Surveillance	**Evaded Surveillance**
The subject consents to the surveillance.	The subject actively avoids surveillance.
Public Security	
Substantial Security Threat	**Little Security Threat**
Credible evidence that lives are at stake.	The pacifist alliance plans to have a bake sale to raise funds.

when do security interests justify invasions of private domains. *See also* Berger v. New York, 388 U.S. 41, 51 (1967).

111. Adapted from the analysis offered by Andrew Jay McClurg, *Bringing Privacy Law Out of the Closet: A Tort Theory of Liability for Intrusions in Public Places*, 73 N.C. L. REV. 989, 1063–67, 1087–88 (1995).

First, if the subject has consented to the surveillance, then the magnitude, context, and security dimensions become irrelevant—such monitoring would be justified. Short of consent, if the magnitude is slight, the context is clearly "public," and the security threat high, the burden of proof for overriding privacy would be low. Sliding to the other extreme, if the magnitude of the invasion is profound, the context clearly "private," and the security threat low, then the burden for overriding privacy would be high. Finally, if there is a substantial security threat backed by clear and credible evidence, then independent of the magnitude, context, or consent, the burden for overriding privacy would be low. For example, if a police officer has good evidence that a murder will take place tomorrow afternoon at a suspect's home, then a warrant would be justified.

In addition, there will be justifiable exceptions to the rule of requiring probable cause and warrants. There may be instances when law enforcement officials need to act quickly and do not have the time to secure a warrant or provide an argument for probable cause—suppose a police officer hears a scuffle and someone shouts for help. Provided that law enforcement officers act in "good faith" and can articulate reasonable grounds for entering private domains after the fact, they should be given some leeway in these cases. Perhaps internal and civilian oversight committees could review such cases to determine if appropriate action was pursued. Thus even in "emergency" situations where privacy is traded for security without a warrant or judicial oversight, we may insist on sunlight provisions and accountability.

Security concerns related to mass transportation or large public gatherings may also justify an exception to the probable cause rule—individuals may be searched without evidence that they will commit a crime in these cases. Nevertheless there are at least two important controls that should be noted. First, individuals in many instances consent to these sorts of minimal intrusions. If you do not want to have your bag searched, then stay home and watch the ballgame on television. Note that the more voluntary the activity, the more robust the consent. Second, in cases where the activity is less voluntary—flying on an airplane for example—we insist on stronger justifications for more intrusive searches. Moreover, judicial and civilian oversight are still appropriate mechanisms for establishing the correct balance between privacy and security in these cases. Few would sanction body cavity searches at airports for the minimal gains in security that could be obtained.

IV. CONCLUSION

While there is still much work to be done, I think that important steps have been taken toward informational privacy rights. Privacy—defined as a control right over access to locations and information—is necessary for human well-being. Individuals who use and possess their own personal information do not necessarily worsen others. Moreover, those who capture, store, and transfer personal information create risks that may worsen information targets. Finally, a presumptive claim to use and control one's own personal information coupled with property rights, body rights, and a general right to make contracts may serve to protect informational privacy.

I have also argued that balancing tests that purport to justify invasions of privacy in the name of security often go awry. "Just trust us," "nothing to hide," and "security trumps" arguments have each been presented and rejected. It has also been argued that in trading privacy for security we should insist on establishing probable cause, judicial oversight, and accountability. Probable cause, in the typical case, sets the standard for when security interests override privacy rights. Judicial oversight, sensitive to case-specific facts like the context and magnitude of the proposed intrusion, introduce an "objective" agent into the process. Sunlight provisions allow for a public discussion of the merits of specific searches and seizures. All of this promotes accountability in that the reasons for a search and the actions of government officials are open to public scrutiny. A further benefit is that such policies engender trust and confidence in public officials.

A transparent society is not inevitable. Privacy at the personal level can be secured through custom and social pressure. Privacy related to big media, corporations, and the state can be guaranteed by law and grounded in customs and social practices. On the other hand, transparency is an important part of good government in the sense that those in power can be held accountable for their actions. Justice William O. Douglas, writing for the dissent in *Osborn v. United States*, 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, but belong to the Government; 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. If a man's privacy can be invaded at will, who can say he is free? If his every word is taken down and evaluated, or if he is afraid every word may be, who can say he enjoys freedom of speech? If his every association is known and recorded, if the conversations with his associates are purloined, who can say he enjoys freedom of association? When such conditions obtain, our citizens will be afraid to utter any but the safest and most orthodox thoughts; afraid to associate

> with any but the most acceptable people. Freedom as the Constitution envisages it will have vanished.[112]

Douglas offers a sobering and frightening prediction of what will ensue if privacy is not tirelessly and vigorously defended. For the sake of freedom, autonomy, and human well-being, we should resist becoming a society of the watchers and the watched.

112. 385 U.S. 323, 353–54 (1966) (Douglas, J., dissenting).