2000

Privacy-as-Data Control: Conceptual, Practical, and Moral Limits of the Paradigm

Anita L. Allen
University of Pennsylvania Carey Law School

Privacy-as-Data Control: Conceptual, Practical, and Moral Limits of the Paradigm

ANITA L. ALLEN*

INTRODUCTION

Professor Paul M. Schwartz's article, *Internet Privacy and the State*,[1] poses two of the most important normative questions contemporary privacy theorists should be asking and attempting to answer. The first question is how, if at all, can we secure meaningful forms of privacy while remaining appropriately accountable to others? The second question is what role, if any, should the state play in the regulation of personal privacy? Professor Schwartz's effort to answer these questions implicitly aims at locating comfortable ground between the polar domains of extreme, unreconstructed liberalism on the one hand and anti-liberal communitarianism or civic republicanism on the other.[2] Schwartz's "liberal" defines privacy as control over personal information and is biased in favor of private sector self-regulation. His "communitarian" and "republican" are deeply skeptical of individual privacy and privacy rights as threats to the common good and civic virtue. Schwartz defends an intermediate stance that falls somewhere between liberalism and communitarianism. Like a liberal, he accepts privacy as a vital good and civil liberty.[3] However, like a communitarian or civic republican, he redefines privacy as what he terms a "constitutive value."[4] Schwartz believes individual privacy protection in some contexts is a paramount public interest, and embraces a degree of state intervention to create and reinforce beneficial privacy norms.[5] Thus, his

* *A.k.a., Anita L. Allen-Castellitto, Professor of Law and Philosophy, University of Pennsylvania School of Law; J.D., Harvard Law School; Ph.D., University of Michigan.*

1. Paul M. Schwartz, *Internet Privacy and the State*, 32 CONN. L. REV. 815 (2000).

2. Professor Schwartz defines his position through a critique of communitarians and republicans, whom he groups together for these purposes, and free market liberals. *See id.* at 836.

3. *Cf.* Pamela Samuelson, *A New Kind of Privacy? Regulating Uses of Personal Data in the Global Information Economy*, 87 CAL. L. REV. 751, 777 (1999) (assessing the implications of Professor Schwartz's desire to treat data protection as a civil liberty).

4. *See* Schwartz, *supra* note 1, at 816.

5. *See id.* at 816-17.

general answer to the first question (about accountability) is that, for the sake of forming a good society and shaping our identities, our society should value privacy and undertake "line-drawing along different coordinates to shape permitted levels of scrutiny."[6] His answer to the second question (about state regulation) is that the state has an affirmative role to play in the correction of information market failures and limiting preference falsification.[7]

I would like to comment on just one important aspect of Professor Schwartz's thoughtful article: his rejection of the popular view that privacy policy should seek to protect individuals' control over personal information.[8] Professor Schwartz observes that the "leading paradigm on the Internet and in the real, or, offline world, conceives of privacy as a personal right to control the use of one's data."[9] According to Schwartz, this privacy-as-data control paradigm (which he calls the "privacy-control" paradigm for short and which I will attempt to clarify below) "seeks to place the individual at the center of decision-making about personal information use."[10] Schwartz was right to take on the privacy-control assumption, for the reasons he gives and for additional reasons I will supply here. I maintain that the popularity of the privacy-control paradigm is problematic because there are a number of conceptual, practical, and moral limits to its plausibility. We liberals—I count myself as one[11]—are attracted to the paradigm because it complements our focus on the interests of individual persons as moral agents, but we must concede its limitations and consider alternatives. After clarifying the privacy-control paradigm in Part I, I will identify its conceptual limitations in Part II, practical limitations in Part III, and moral limitations in Part IV. I conclude, with Professor Schwartz, that alternatives to the privacy-as-data control paradigm are needed to guide our urgent philosophical and policy understandings of privacy and its protection in the age of the Internet.

I. UNDERSTANDING THE PRIVACY-CONTROL PARADIGM

In a book aimed at the lay public, Ann Cavoukian and Don Tapscott identity several understandings of privacy but assert that: "An important component of protecting privacy is maintaining control over information

6. *Id.* at 834.
7. *See id.* at 817.
8. *See id.* at 816.
9. *Id.* at 820.
10. *Id.*
11. *See* Anita L. Allen, *Coercing Privacy*, 40 WM. & MARY L. REV. 723 (1999) [hereinafter Allen, *Coercing Privacy*]; *see also* ANITA L. ALLEN, UNEASY ACCESS: PRIVACY FOR WOMEN IN A FREE SOCIETY (1988) [hereinafter ALLEN, UNEASY ACCESS].

that is circulating about you—informational privacy."[12] The view that privacy is importantly or essentially about control over personal information is promulgated in recent publications aimed at scholars and professionals.[13] Focusing on current efforts to design policies that accommodate informational privacy concerns in cyberspace, Professor Schwartz concludes that the "leading paradigm on the Internet and in the real, or offline world, conceives of privacy as a personal right to control the use of one's data."[14] He calls this paradigm "privacy-control" and describes the "weight of the consensus about the centrality of privacy-control" as "staggering."[15] In framing the problematic privacy-control paradigm for his critique, Schwartz understands the paradigm to encompass a set of views about the definition of "privacy," requirements of the "right to privacy," and the ideal aims of privacy policy. In this section, I would like to clarify the parameters of the privacy-control paradigm with which Schwartz takes issue and the extent of its popularity.

Adding precision to Schwartz's presentation of the paradigm, I want to suggest that the paradigm he identifies is comprised of three complex, distinguishable, and severable notions. They are, first, the notion that the term "privacy" *means* control (or rights of control) over the use of personal data or information; second, the notion that the expression "right to privacy" *means* the right or claim to control the use of personal data or information; and, third, the notion that the central aim of privacy regulation should be promoting individuals' control (or rights of control) over personal data or information. When I say that each notion is complex, I mean that each of the three is amenable to detailed analysis that would reveal ambiguities too subtle to interest most lawyers. When I say that each is distinguishable, I mean that each one is a semantically distinct proposition from the other two. And when I say that each is severable, I mean that, while logically consistent with the others, neither notion logically entails the other two. So, for example, a person who believes that "privacy" means data control might also believe, with complete logical consistency, that privacy regulation should not have as its central aim promoting individuals' control over personal data or information. Moreover, a person who believes that "privacy" means data control and that "the right to privacy" means the right to data control, is not logically committed to the beliefs that there is or should

12. ANN CAVOUKIAN & DON TAPSCOTT, WHO KNOWS: SAFEGUARDING YOUR PRIVACY IN A NETWORKED WORLD 9 (1997).

13. *See, e.g.*, Jerry Berman & Deidre Mulligan, *Privacy in the Digital Age: Work in Progress*, 23 NOVA L. REV. 549, 557 n.11 (1999). To that end, the authors rely on Alan Westin's much-quoted definition of privacy as control over information in his work *Privacy and Freedom*. *See generally* ALAN WESTIN, PRIVACY AND FREEDOM (1967); *see also* LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 143 (1999) ("Privacy, as Ethan Katsh defines it, is the power to control what others can come to know about you.").

14. Schwartz, *supra* note 1, at 820.

15. *Id.*

be a right to privacy, and that privacy regulation should aim at rationally optimizing or otherwise promoting "informational self-determination through individual stewardship of personal data."[16]

The three aforementioned data-control notions form a paradigm because they are complementary, not because they are mutually entailing. They are complementary in the significant sense that, individually and as a group, they cohere with liberal moral, political, and legal perspectives that emphasize wide sway for individual autonomy. However, the data-control paradigm is neither necessarily embraced in full by all liberals, nor rejected in full by all non-liberals. As explained below, a liberal could reject a definition emphasizing data control in favor of a broader definition of "privacy" or of the "right to privacy."[17] In addition, a liberal might easily reject individual data control as the *central* goal of privacy policy in key regulatory regimes, such as laws regulating medical or financial information. Finally, a non-liberal could also hold the notion that "privacy" means data control. Indeed, a communitarian could agree with a liberal that "privacy" means control of personal data, but disagree about what rights of privacy to recognize and what level of privacy protection society ought to afford.

Schwartz asserts that the consensus about the privacy-control paradigm is "staggering." I, too, am struck by the proliferation of the paradigm in the privacy literature spawned by cyberspace. Yet, there is less overall consensus among privacy theorists than Schwartz acknowledges about at least one of the three notions comprising the paradigm. When it comes to the meaning or definition of "privacy" there is not as much consensus about the identification of privacy with control over information as Schwartz represents.[18] On the contrary, there is no universally accepted philosophical definition of "privacy." I attribute wide variation in definitional accounts of privacy "to the confluence of three factors: (a) variation in the use and denotational and connotational meanings of 'privacy;' (b) variation in the purposes for which definition of 'privacy' is undertaken; and (c) variation in approaches taken to the task of definition itself."[19]

To be sure, a number of prominent policy analysts and theorists employ the idea of control in their definitions of what privacy and the right to privacy mean. Sometimes the term "control" is used expressly in a definition of privacy, as where Charles Fried describes privacy as "control we

16. *Id.*

17. *See infra* note 28 and accompanying text.

18. *Cf.* Simon G. Davies, *Re-Engineering the Right to Privacy: How Privacy Has Been Transformed from a Right to a Commodity*, *in* TECHNOLOGY AND PRIVACY: THE NEW LANDSCAPE 153 (Philip E. Agre & Marc Rotenberg eds., 1997) ("The pursuit of a single definition of privacy has preoccupied so many travelers in this field that the quest has become a standard challenge in the privacy field.").

19. ALLEN, UNEASY ACCESS, *supra* note 11, at 5.

have over information about ourselves."[20] Sometimes the concept is present without the term, as where Alan Westin wrote of the "claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others."[21] The concept of control even figures into accounts of privacy that go beyond informational privacy to include physical, decisional, and proprietary senses of the term. Hence, Richard Parker characterized privacy as "control over who can sense us,"[22] and Tom Gerety defined privacy as "autonomy or control over the intimacies of personal identity."[23] Since definitions of privacy vary with the purpose for definition,[24] these largely liberal-minded legal, social, and moral theorists defined privacy in terms of control to complement their further view that just government and ideal social practices should promote individual control over personal data. As previously noted, communitarian critics of liberalism and liberal conceptions of privacy might also define privacy as individual control over personal information, for purposes of emphasizing the privacy sacrifices of accessibility and disclosure demanded of participation in responsible communities.

II. THE CONCEPTUAL LIMITS OF THE DATA-CONTROL PARADIGM

One must acknowledge that many theorists have flatly rejected definitions of "privacy" that equate privacy with control over personal data.[25] While some of the theorists who reject the control-emphatic definition have done so as part of an effort to supplant liberalism, even liberals have rejected control-based definitions of "privacy." Theorists reject defining "privacy" as control or rights of control for a number of reasons that point to the conceptual limitations of the entire privacy-control paradigm itself.

For starters, some theorists, including liberal theorists, reject the notion that "privacy" is best defined as a right, viewing it instead as a claim of right.[26] Others reject defining privacy as either a right or a claim of right,

20. Charles Fried, *Privacy*, 77 YALE L.J. 475, 482 (1968).

21. WESTIN, *supra* note 13, at 7.

22. Richard B. Parker, *A Definition of Privacy*, 27 RUTGERS L. REV. 275, 281 (1974).

23. Tom Gerety, *Redefining Privacy*, 12 HARV. C.R.-C.L. L. REV. 233, 236 (1977).

24. *See* ALLEN, UNEASY ACCESS, *supra* note 11, at 6.

25. They have similarly rejected definitions that define privacy as control over routes of observation, control over routes of accessibility, control over decision-making, and control over identity. *See* ALLEN, UNEASY ACCESS, *supra* note 11, at 18.

26. *Cf.* Ruth Gavison, *Privacy and the Limits of Law*, *in* PHILOSOPHICAL DIMENSIONS OF PRIVACY: AN ANTHOLOGY 346, 348-49 (Ferdinand David Schoeman ed., 1984) [hereinafter PHILOSOPHICAL DIMENSIONS OF PRIVACY] (asking whether "privacy [is] a right, a claim, a form of control, a value?" and answering that it is a "neutral" state of affairs).

arguing that privacy is a set of cultural values and practices.[27] Still others present privacy as a factual condition or state of affairs that rights of privacy, privacy claims, and cultural practices potentially protect.[28]

Theorists also reject control-based definitions on the ground that they are too narrow. These theorists insist on defining "privacy" broadly, to better capture patterns of actual usage. The actual contemporary usage of "privacy" in the United States is particularly broad. "Privacy" can mean informational privacy, but also physical, informational, and proprietary privacy.[29] When Americans describe abortion rights, the right to die, and gay rights as protective of privacy they are not just talking about the right to control personal data. They are talking about a degree of freedom from unwanted intervention, decisional autonomy, and freedom of choice generally. When Americans say they want "privacy" they may be interested in conditions of solitude, the need for repose, or the seclusion needed for intimacy rather than control over facts about themselves. Data control as a general definition of "privacy" is implausible because it simply ignores common meanings. As a stipulative definition or a description of what many people worry about in the context of online communications, "data control" has more plausibility. However, even for purposes of discussing issues in cyberspace, there appear to be good reasons for rejecting control-emphatic definitions of privacy. A concept other than control may more adequately capture the sense of "privacy" at issue in online contexts. One such candidate is the concept of inaccessibility.

An examination of the philosophical literature that seeks to define privacy and its value reveals that the privacy-as-control definitions so popular with the data protection community are not the kinds of definitions of privacy that have attracted the largest following among philosophers.[30] In-

27. *See* Jeffrey Reiman, *Privacy, Intimacy, and Personhood*, *in* PHILOSOPHICAL DIMENSIONS OF PRIVACY, *supra* note 26, at 300, 310 ("Privacy is a social practice. It involves a complex of behaviors . . . .").

28. I include myself in this group. *See generally* ALLEN, UNEASY ACCESS, *supra* note 11, Chapter 1.

29. I distinguish and elaborate these four dimensions of privacy. *See* Anita L. Allen, *Genetic Privacy: Emerging Concepts and Values*, *in* GENETIC SECRETS: PROTECTING PRIVACY AND CONFIDENTIALITY IN THE GENETIC ERA 31, 34 (Mark A. Rothstein ed., 1997) (Briefly, informational privacy concerns are about access to personal information; physical privacy concerns are about access to persons and personal spaces; decisional privacy concerns are about governmental and other third-party interference with personal choices; and proprietary privacy concerns are about the appropriation and ownership of interests in human personality.).

30. *See* ALLEN, UNEASY ACCESS, *supra* note 11, at 11. As I have written:

> Restricted-access definitions have identified privacy with a limitation on others' access to the individual; the condition of being protected from unwanted access by others; lack of access to information related to intimacies; selective control over access to oneself or one's group; an existential condition of limited access to an individual's life experiences and engagements; the state of limited access by others to certain modes of being in a person's life; a limitation on access of one or more entities to an entity that possesses experiences; and as the exclusive access of a person to a realm of his own. Privacy as a political ideal has been interpreted in restricted access terms as an individual's freedom to secure conditions free

deed, as recently as a dozen years ago, definitions emphasizing accessibility and inaccessibility were arguably more pervasive than control-based definitions. On these theories, other than in contexts in which "privacy" holds its decisional and proprietary meanings, privacy refers to a degree of inaccessibility of a person or information about her to others' five senses and surveillance devices. I have been an advocate of such a view in the past.[31]

The best conceptual reason for rejecting characterizations of privacy that emphasize control may be that control over personal data appears to be neither necessary nor sufficient for states of privacy to obtain. Suppose people had perfect control over personal data about themselves. Would they necessarily have privacy? The answer is surely no. Having control over personal information does not mean having privacy. The person in control of her data might elect to share personal information with others. We have seen a lot of this in the age of cyberspace. For example, a couple announced plans to lose their virginity live over the Internet to underscore its special importance to them.[32] A nurse chose to broadcast her double mastectomy live over the Internet to educate the public about breast cancer.[33] A married woman choose to share the delivery of her third child with other expectant parents by delivering her baby live over the Internet.[34] Women have chosen to use "adult entertainment" Web sites to sell images of themselves engaging in sexual intercourse or sexually explicit fantasies.[35] Like "Jenni," men and women have chosen to train Web video cameras on the interiors of their dwellings and then sell or give away real-time images of their daily lives.[36]

---

from unwanted access. The concept of private affairs has been explained as being those activities and concerns of an individual that ought to be protected by limited access. Finally, group privacy has been defined in terms of restrictions on others' access to one's group.

Id. at 11 (footnotes omitted).

In the intervening ten years, some philosophers of privacy have been critical both of control and access oriented understandings of privacy. *See, e.g.*, PATRICIA BOLING, PRIVACY AND THE POLITICS OF INTIMATE LIFE (1996); JULIE C. INNESS, PRIVACY, INTIMACY, AND ISOLATION (1992).

31. *See* ALLEN, UNEASY ACCESS, *supra* note 11, at 3.

32. *See* Don Feder, *Innocence Lost in Net Fishbowl*, BOSTON HERALD, July 22, 1998, at 029, *available in* LEXIS, News Library, Bherald File.

33. *See As Part of Breast Cancer Awareness Month, the Health Network Will Webcast Live Mastectomy and Breast Reconstruction Surgery*, HEALTH NETWORK (Oct. 13, 1999) <http://www.ahn.com/Press_Release/press_display.asp?idocid=4667>.

34. In June 1998, a woman who revealed her name only as "Elizabeth" gave birth live over the Internet to "Baby Sean" in the Arnold Palmer Hospital in Orlando, Florida. The mother declared her motives to be public education. *See* Ellen Goodman, *Internet Birth a Blow to Privacy*, BUFFALO NEWS, June 20, 1998, at 3C, *available in* LEXIS, News Library, Bufnews File.

35. *See* Jack Boulware, *Web Rouser: Former Lusty Lady Dancer Caity McPherson Struggles to Make a Living on the Oversexed Internet*, NEW TIMES SF WKLY., Mar. 31, 1999, *available in* LEXIS, News Library, New Times SF Wkly. File; Michael Saunders, *Web's Red-light District Shines in Technology, Profits*, BOSTON GLOBE, May 4, 1998, at C7, *available in* LEXIS, News Library, BGlobe File.

36. *See* Jennicam (visited Nov. 16, 1999) <http://www.jennicam.com>. The initial screen of the Web site, visited November 16, 1999, reads like a dictionary entry which defines Jennicam as "a real-

Jenni's Web stardom provides a good illustration of the disconnection between privacy and data control. Because Jenni is free to turn her camera off and close down her Web site, she is free to exercise the partial capacity she shares with most other Americans to control access to personal information about the details of her home life and, to that extent, to restore her privacy. But as long as the camera is feeding images of her to others and others are watching, she has no physical privacy to speak of, and others possess otherwise private information about her home life. That Jenni has control of the camera does not mean that she has privacy. In fact, what makes Jenni, Ana, and similar web performers popular is the fascination we have with people who are willing to forego the usual domestic privacies for public amusement or reflection. Control is not sufficient for privacy, nor is it necessary. A prison inmate locked in solitary confinement has privacy—too much of it—but no control over personal information, since prison officials can enter his quarters or perhaps access surveillance camera images of him at will.[37] The kind of mandatory privacy the inmate experiences is not a form of privacy most people would want for themselves. Yet most of us approve of at least some forms of punitive or disciplinary solitary confinement in the context of criminal corrections, and sometimes voluntarily isolate ourselves from others.

Defining "privacy" as data control directs our attention to the questions of consent and choice.[38] But if what people in control are choosing and consenting to is making themselves informationally and physically more accessible to others, the states of affairs they are bringing about are not privacy, but the opposite of privacy. Physical and informational privacy

---

time look into the real life of a young woman" and "an undramatized photographic diary for public viewing esp. via Internet." *Id.* The site claims that cameras show the bedrooms, living room, and dining room of Jenni's home, and promises a roving camera soon. Jennicam membership costs $15 for a 12-month subscription. Non-members can visit the Jennicam Gallery, a sample of images, showing photographs of Jenni's feet, eyes, nude back, and torso, plus Jenni bathing, caressing a lover in bed, entertaining a gathering of friends, and working at her desk.

37. Compare what Ferdinand Schoeman has written:

> Privacy has been identified also as the measure of *control* an individual has over: 1. information about himself; 2. intimacies of personal identity; or 3. who has sensory access to him. . . . [This definition] presents some difficulties. . . . [It] . . . seem[s] particularly vulnerable to a number of counterexamples. We can easily imagine a person living in a state of complete privacy but lacking control over who has access to information about him. . . . To take another example, a person who chose to exercise his discretionary control over information about himself by divulging everything cannot be said to have lost control, although he surely cannot be said to have any privacy.

Ferdinand Schoeman, *Philosophical Dimensions of the Literature*, *in* PHILOSOPHICAL DIMENSIONS OF PRIVACY, *supra* note 26, at 1, 2-3; *cf.* CHARLES J. SYKES, THE END OF PRIVACY 19 (1999) ("Both the prison and the concentration camp deprive inmates of freedom, but the tearing away of every shred of privacy is what deprives them of dignity and causes them to surrender their hold of the sense of self.").

38. It also draws our attention to the concept of "data," which invites us to conceive of personal information from the distinctively utilitarian perspective of one for whom the information has value only to the extent that it can be packaged in standardized and bureaucratically manipulable formats.

entail a degree of inaccessibility.[39] Informational privacy obtains where information actually exists in a state of inaccessibility, whether it is locked in a file drawer, computer, or in someone's mind. Anonymity, confidentiality, reserve, and secrecy—not merely having the choice to bring these about—are forms of privacy. People who could enjoy privacy and are in control of personal information are choosing to give up privacy. It is for this reason that commentators troubled by people deciding to broadcast otherwise intimate or confidential conduct over the Internet have begun to ask the question whether it is possible to invade your own privacy.[40] You can invade (that is diminish) your own privacy the same way you can diminish your own freedom. In the era of slavery, it was not said that the free man who sold himself into slavery remained free because servitude was his choice, and we should not say that a private person who voluntary gives up privacy remains private. And just as the moral and policy implications of voluntary servitude have troubled us, so too, should the moral and policy implications of voluntary loss of privacy.

III. THE PRACTICAL LIMITS OF THE DATA-CONTROL PARADIGM

To the argument in Part II that conceptual limitations burden the privacy-control paradigm, I now add the argument that there are practical limits. In explaining conceptual limits, I focused on the privacy-control paradigm's definitional notion that "privacy" means data control, and suggested that privacy is open to broader and more perspicacious definitional analysis, as the philosophical literature reflects. In explaining practical limits, I begin by focusing on the privacy-control paradigm's notion that rights of privacy are rights of data control. Here, I suggest that Professor Schwartz's concerns about whether people can actually control personal data are well-taken. It is pointless (or merely symbolic) to ascribe a right to data control if it turns out that exercising the right is impossible.

Professor Schwartz stresses the practical difficulties attending the notion that controlling personal data is the basis of a meaningful right, in cyberspace or offline. Control over personal information is an illusion, he argues. Typical Internet users disclose a great deal of information.[41] They do so directly and knowingly as they purchase goods and services or send e-mail. They do so less directly and knowingly as their travels through cyberspace deposit cookies,[42] and as firms with whom they do business

39. *See* ALLEN, UNEASY ACCESS, *supra* note 11, at 13-18.

40. *See* Margaret Talbot, *Candid Camera*, NEW REPUBLIC, Oct. 26, 1998, *available in* LEXIS, News Library, Newrpb File.

41. *See generally* THOMAS A. PETERS, COMPUTERIZED MONITORING AND ONLINE PRIVACY 196-310 (1999).

42. As Reginald Whitaker has written:

pass personal data about their customers to third party or successor organizations. Professor Schwartz thus argues that Internet users as a class do not control personal data because they are uninformed about all the ways their data can be collected from them as they negotiate cyberspace, and because they are powerless to demand meaningful limits on third party disclosures. Schwartz argues that, because of the unreliable and adhesive nature of privacy agreements, even people using sites that offer opportunities to preauthorize or refuse data collection and third-party disclosures, or that give notice of such practices, do not control personal information.

Schwartz's argument has particular force with respect to features of the Internet that are not amenable to improvement. However, some of the barriers to greater individual control over personal data are in principle amenable to remedy. As people become better educated about Internet use, they will be empowered to engage in self-help, such as disabling cookies.[43] So-called "privacy enhancing technologies" (PETS) could help us build privacy protection into the architecture of the Internet.[44] It may be possible to protect informational privacy through technologies that conceal identity and information while allowing transactions to take place.

But, according to Professor Schwartz, even if it were possible to educate and empower people for data control, there would still be a reason to reject the idea of a right to control personal. People do not and cannot control personal data because, first, there are too many other people using data about us to whom each of us is accountable for information (such as insurers); and, second, the information demands of bureaucratic efficiency (such as those of insurers) override individuals' desire for privacy. Schwartz intends this last argument against the second notion of the privacy-control paradigm to apply to the offline as well as the online world.

> Among the more interesting cyber-surveillance techniques are "cookies." Net users who register with cites or download software have cookies placed directly on their hard drives. Cookies are strings of numbers that identify the user to the merchant. They speed up the process of doing business. For instance, if I register to subscribe to a service, a cookie implanted in my computer automatically re-registers me each time I enter the site, obviating a time consuming process of entering identification and remembering a password. . . . However convenient, cookies . . . are a key to gaining remote access to personal computer hard drives, with frightening potential for abuse.

REGINALD WHITAKER, THE END OF PRIVACY: HOW TOTAL SURVEILLANCE IS BECOMING A REALITY 103 (1999).

43. *See id.* at 103 ("As awareness of the potential dangers of cookies has risen, various defenses have been made available. "Cookie cruncher" programs remove cookies from a hard drive. And Net browsers like Netscape give users the option to refuse all cookies, or be warned in advance that an action will initiate a cookie, or be warned each time an existing cookie is about to be activated.").

44. Colin J. Bennett & Rebecca Grant, *Introduction, in* VISIONS OF PRIVACY: POLICY CHOICES FOR THE DIGITAL AGE 9-10 (Colin J. Bennett & Rebecca Grant eds., 1996) [hereinafter VISIONS OF PRIVACY] (citing views of Janlori Goldman and Ann Cavoukian). According to Goldman, "[t]he rise of technologies that empower Internet users affirmatively to express control over personal information can fundamentally shift the balance of power between the individual and those seeking personal information." *Id.* at 98.

Schwartz's case against the right to control data has both a practical argument—privacy is inefficient—and a moral side—privacy is irresponsible. Even if data control were possible and practical, it could be argued that for moral reasons people ought not to be ascribed a right to data control, and that enhancing individual control over personal data is not morally worthy as a central objective of privacy regulation.

IV. THE MORAL LIMITS OF THE DATA-CONTROL PARADIGM

The privacy-control paradigm can obscure that in so many policy contexts it is wrong to insist on individual control over personal data. One policy concern is that people will want too little privacy. That is, that they will use rights of data control to give up forms of privacy deemed vital to their interests. This concerns militates against designing privacy policies focused solely on enhancing control over personal data by individuals. Doing so may be neither in their interests nor in the interests of the greater society. Liberals have generally assumed that privacy is something people want and that the main goal of public policy is to enhance their capacity to get what they want. This effort to maximize choice is problematic though, if it turns out that people are choosing to give up more privacy than is consistent with liberal conceptions of the person or the liberal way of life.

Unless people want privacy, neither government nor private sector policies aimed at individual data control and individual stewardship of personal information can insure privacy. People who ascribe to legal rights and entitlements to control personal data may choose to share more data than they conceal. They may prefer disclosure for the sake of monetary profit, artistic creation, public education, medical care, commercial transactions, entertainment, or community. Policy-makers may proceed on the basis of one of two assumptions: (1) the anti-paternalist assumption that personal privacy is a good only to the extent that people want it (and therefore that it should not be forced on people); or (2) the paternalist assumption that personal privacy is a good, even for those who do not want it (and therefore that efforts should be made to alter preferences or to coerce privacy). The idea of "coercing privacy" sounds strange, but is really quite familiar.[45] Certain laws already mandate privacy, such as the (popular) laws that require that clothing be worn in public places and the (much criticized) regulations that prohibit military service members from disclosing their sexual orientation. The building codes that regulate the design and placement of residential housing also mandate privacy. A Manhattan builder does not have the option of constructing an apartment building entirely of transparent glass. Many social norms that fall short of law that once coerced privacy have eroded in recent years, giving way to openness

45. *See generally* Allen, *Coercing Privacy*, *supra* note 11, at 723.

about matters of health, sexuality, and opinion. The culture of "exhibitionism and voyeurism" is evidence of this erosion. To aggressively protect privacy, policy-makers may be required to adopt policies that require certain privacies, want them or not. They may be required to undertake the formative project of creating citizens who want certain personally and socially beneficial forms of privacy.

The privacy-control paradigm obscures the need for concern that people will want too little privacy, and also the concern that people will want too much privacy. A sense of moral responsibility for one's conduct and a desire for morally responsive public policies might lead to abandonment of enhancing individual data control as the central objective of privacy policy. For example, the demands of responsible employment place a moral limit on policies that might purport to give workers greater control over personal financial and health information. To take another example, it might seem innocuous to make the assertion that people should be able to control personal financial data, until one realizes that our political obligations to our country and fellow citizens make that impossible. As James Rule and Lawrence Hunter have observed, "if governments are expected to tax income or commerce . . . citizens can hardly expect control over information about their personal finances."[46] It would seem unwise to prohibit the constitutionally mandated decennial census-takers from collecting personal information about household income. Welfare, Social Security, disaster relief, student loans—all of these public benefits should be available, but surely require moral accountability in the form of personal financial disclosures.

The area of health care delivery and medical record privacy is a good one to examine for purposes of exposing the weaknesses of a privacy-control paradigm. Medical privacy is important. Many people have felt a need to conceal their bodies and information about the condition of their bodies and minds, particularly when they are ill and aging. Moreover, it is important to many people that they or someone they designate make some of the key decisions about the context and scope of health care and disclosures. The central aim of medical record policy cannot be to give individuals complete control over medical information. Information sharing is a sine qua non of modern health care delivery, and also a bureaucratic requirement of insurance. The twin demands of confidential disclosure to health providers and accountability to insurers entail that the individual cannot control personal medical data once he or she decides to seek professional care. To speak of controlling medical data is also problematic because of the difficulty of concealing health matters from family, friends, co-workers, and even strangers. If a woman discovers a lump in her breast,

46. James Rule & Lawrence Hunter, *Towards Property Rights in Personal Data*, *in* VISIONS OF PRIVACY, *supra* note 44, at 168, 169-70.

she can control the time and place that information about her tumor is shared with others. However, the list of medical conditions that are plainly visible to others is extremely long: alcoholism, jaundice, Alzheimer's, Parkinson's, psoriasis, deafness, tuberculosis, and skin cancer cannot be concealed. The interests we have in medical privacy are best addressed by focusing less on the misleading ideal of controlling medical information, and more on the wider concerns of, first, the social norms of civility, respect and responsibility (that help us manage the medical information we possess about ourselves and others), and second, fair information practices[47] (such as informed consent, patient access to records, limited dissemination by providers and insurers, and the accuracy and security of records and systems of records, that health providers, insurers and others ethically and accountably gather, maintain, and share personal information entrusted to them).

These moral qualms about the "privacy control" paradigm do not entail that complete custody of personal data should be uncritically yielded in every case to police and government agencies. Nor do moral qualms about the importance of willingness to share information entail that e-commerce should be conducted with no attention to consumer information privacy interests. However, they are meant to suggest that because personal information cannot and should not be substantially controlled by individuals, privacy enhancing technologies should be thought of as just that privacy enhancing, not privacy controlling, technologies. They are also meant to suggest that because it is both misleading and wrong to hold up "privacy control" as such a policy aim, something very different and more complex than data-control is the realistic aim of e-commerce and marketing privacy policies. Precisely defining this "something very different" is one of the most challenging tasks on the table for privacy policy theorists. Professor Amitai Etzioni is content to call it balancing individual and entity interests in light of the common good.[48] Professor Schwartz tries to get at this alternative to data control when he points to the need to think of privacy constitutively and to understand that respect for it requires contextual line-drawing.

What would Schwartz's suggested approach look like in practice? I imagine this. Consider the case *Wine Hobby USA, Inc. v. United States IRS*.[49] Wine Hobby was the seller and distributor of avocational equipment for the making of wine. The company wished to market its products to an

47. *See* Mary J. Culnan & Robert J. Bies, *Managing Privacy Concerns Strategically: The Implications of Fair Information Practices for Marketing in the Twenty-First Century*, *in* VISIONS OF PRIVACY, *supra* note 44, at 6, 149 (introduction listing the fair information practices about which there is emerging international consensus, and article elaborating an expansive understanding of such policies).

48. *See* AMITAI ETZIONI, THE LIMITS OF PRIVACY (1999).

49. 502 F.2d 133 (3d Cir. 1974).

individual wine hobbyist, and filed a Freedom of Information Act (FOIA)[50] request for a copy of the list of persons registered (as required by law) with the Bureau of Alcohol, Tobacco and Firearms as producers of wine for "family use." The government responded, claiming that the information could not be disclosed because of Exemption 6 of the Act, which excludes from the coverage of the Act "personnel and medical and similar files the disclosure of which would constitute a clearly unwarranted invasion of privacy."[51] The court found for the government. It did not, however, assert that citizens have a right to control personal information, rather, it described the need to balance competing interests. In explicating the family wine-makers' privacy interests, the court focused on American cultural traditions of family and domestic privacy—that is, on constitutive privacy norms. The idea that citizens have an absolute right to control personal information is contradicted by the mandatory government wine production reporting requirement itself. The government's registration regulation denied persons a right to control information sufficient to exclude government. However, the family-privacy protecting interpretation of FOIA in this case construes government as a confidant rather than a broadcaster. The sense of privacy is offended by having others load our mailboxes with solicitations and advertisements based on information about our habits and avocations obtained as a result of a mandatory reporting requirement. The government that makes us accountable for taxation due on potentially lucrative wine production also limits access to personal information that we yield reluctantly and for which others have considerably less than a compelling need. Important to a constitutive conception of privacy is what Schwartz calls the "pattern of knowledge" represented by public disclosure of registered family wine producers' identities to third parties intending commercial usage. Although our common identities as participants in a free and open society support the goal of open records embodied in FOIA, and our needs as a market economy include cheap information, the boundary around the family home endorsed by the court is also one Schwartz could support. For while it is Professor Schwartz's view that we must avoid the "data fortress that isolates personal information in some absolute sense,"[52] we also must avoid a way of life that turns our desire to know what government is up to into a way of life that will permit fellow citizens to know what we as law-abiding citizens are up to in our homes and family lives.

50. Freedom of Information Act, 5 U.S.C. § 552 (Supp. III 1997).

51. *Id.* §552(b)(6) (exception for personnel and medical and similar files).

52. Schwartz, *supra* note 1, at 834.

V. CONCLUSION

The appeal of the privacy-control paradigm is the appeal of the idea that privacy protection, virtually by definition, is all about vesting control over personal information in the individual. I have attempted to clearly outline the conceptual, practical, and moral limits of the privacy-control paradigm that embodies this facially appealing idea. I elaborated the paradigm as consisting of the three severable notions that "privacy" means personal data control or rights of data control; that the right of privacy is a right of personal data control; and that enhancing personal data control by individuals is the optimal end of privacy regulation. Recognition of the limits of the paradigm must lead serious adherents to respond with efforts to repair or replace it.