Governance Studies at BROOKINGS

April 01, 2011

Reuters/Bazuki Muhammad - A general view of the Global Response Centre of the International Multilateral Partnership Against Cyber Threats in Cyberjaya.

Databuse: Digital Privacy and the Mosaic

Benjamin Wittes

INTRODUCTION

The question of privacy lies at, or just beneath, the surface of a huge range of contemporary policy disputes. It binds together the American debates over such disparate issues as counter-terrorism and surveillance, online pornography, abortion, and targeted advertising. It captures something deep that a free society necessarily values in our individual relations with the state, with companies, and with one another. And yet we see a strange frustration emerging in our debates over privacy, one in which we fret simultaneously that we have too much of it and too little. This tendency is most pronounced in the counter-terrorism arena, where we routinely both demand—with no apparent irony—both that authorities do a better job of "connecting the dots" and worry about the privacy impact of data-mining and collection programs designed to connect those dots. The *New Republic* on its cover recently declared 2010 "The Year We Were Exposed" and published an article by Jeffrey Rosen subtitled "Why Privacy Always Loses."[1] By contrast, in a book published earlier in 2010, former Department of Homeland Security policy chief Stewart Baker described privacy concerns as debilitating counter-terrorism efforts across a range of areas:

> even after 9/11, privacy campaigners tried to rebuild the wall [between intelligence and law enforcement] and to keep DHS from using [airline] reservation data effectively. They failed; too much blood had been spilled. But in the fields where disaster has not yet struck—computer security and biotechnology—privacy groups have blocked the government from taking even modest steps to head off danger.[2]

Both of these theses cannot be true. Privacy cannot at once be always losing—a value so at risk that it requires, for so Rosen contends, "a genuinely independent [government] institution" dedicated to its protection—and be simultaneously impeding the government from taking even "modest steps" to prevent catastrophes.

Unless, that is, our concept of privacy is so muddled, so situational, and so in flux, that we are not quite sure any more what it is or how much of it we really want.

In this paper, I explore the possibility that technology's advance and the proliferation of personal data in the hands of third parties has left us with a conceptually outmoded debate, whose reliance on the concept of privacy does not usefully guide the public policy questions we face. And I propose a different

Benjamin Wittes is a senior fellow and research director in Public Law at the Brookings Institution. He is also a co-founder of the *Lawfare* blog and has written extensively on the relationship between law and security.

[1] Jeffrey Rosen, *Nude Breach*, THE NEW REPUBLIC, Dec. 13, 2010, *available at* http://www.tnr.com/article/magazine/79750/nude-breach-privacy-americans. Rosen's answer is bureaucratic: "[P]rotecting privacy isn't something that the U.S. government has ever done well. Compared to their European counterparts, U.S. privacy offices lack both independence and regulatory teeth. . . . [T]he government needs a genuinely independent institution dedicated to protecting Americans' privacy. . . ." *Id.*

[2] STEWART BAKER, SKATING ON STILTS 309-320 (2010).

vocabulary for that debate—a concept I call "databuse." When I say here that privacy has become obsolete, to be clear, I do not mean this in the crude sense that we have as a society abandoned privacy in the way that, say, we have abandoned once-held moral anxieties about lending money for interest. Nor do I mean that we have moved beyond privacy in the sense that we moved beyond the need for a constitutional protection against the peacetime quartering of soldiers in private houses without the owner's consent.[3] Privacy still represents a deep value in our society and in any society committed to liberalism.

Rather, I mean to propose something more precise, and more subtle: that the concept of privacy as we have traditionally understood it in law no longer describes well or completely the actual value at stake in the set of issues we continue to argue in privacy's name. The notion of privacy was always vague and hard to pin down as an operational matter in law. But this problem has grown dramatically worse as a result of the proliferation of data about all of us and the ability to analyze and cross-reference that data systematically and instantly. To put the matter bluntly, the concept of privacy will no longer bear the weight we are placing upon it. And because the term covers such a huge range of ground, its imprecision with respect to these new problems creates great indeterminacy as to what the value we are trying to protect really is, whether it is gaining or losing ground, and whether that is a good thing or a bad.

In this paper, I examine privacy's conceptual obsolescence with respect only to a single area, albeit one that is by itself hopelessly sprawling: data about individuals held in the hands of third parties. Our lives, as I have elsewhere argued, are described by a mosaic of such data—an ever-widening array of digital fingerprints reflecting nearly all of life's many aspects. Our mosaics record our transactions, our media consumption, our locations and travel, our communications, and our relationships. They are, quite simply, a detailed portrait of our lives—vastly more revealing than the contents of our underwear drawers yet protected by a weird and incoherent patchwork of laws that reflect no coherent value system.[4] We tend to discuss policy issues concerning control over our mosaics in the language of privacy for the simple reason that privacy represents the closest value liberalism has yet articulated to the one we instinctively wish in this context both to protect and to balance against other goods—goods such as commerce, security, and the free exchange of information. And there is no doubt an intuitive logic to the use of the term in this context. If one imagines, for example, the malicious deployment of all of the government's authorities to collect the components of a person's mosaic and then the use of those components against that person, one is imagining a police state no less than if one imagines an unrestricted power to raid people's homes. If one imagines the unrestricted

[3] U.S. CONST. amend. III.

[4] *See* BENJAMIN WITTES, WELLS C. BENNETT & RABEA BENHALIM, RATIONALIZING GOVERNMENT COLLECTION AUTHORITIES: A PROPOSAL FOR RADICAL SIMPLIFICATION (2011), http://www.brookings.edu/topics/justice-and-law.aspx.

commerce in personal information about people's habits, tastes, and behaviors—innocent and deviant alike—one is imagining an invasion of personal space as destructive of a person's privacy as the breaking into that person's home and the selling of all the personal information one can pilfer there.

Yet the construction of these issues as principally implicating privacy is not inevitable; indeed, privacy itself is not inevitable as a legal matter. It was, as I shall argue, created in response to the obsolescence of previous legal constructions designed to shield individuals from government and one another, and it was created because technological developments made those earlier constructions inadequate to describe the violations people were feeling. Ironically, today it is privacy itself that no longer adequately describes the violations people are feeling with respect to the mosaic—and it describes those violations less and less well as time goes on. Much of the material that makes up the mosaic, after all, involves records of events that take place in public, not in private; driving through a toll booth or shopping at a store, for example, are not exactly private acts. Most mosaic data is sensitive only in aggregation; it is often trivial in and of itself—and we consequently think little of giving it, or the rights to use it, away. Indeed, mosaic data by its nature is material we have disclosed to others, often in exchange for some benefit, and often with the understanding, implicit or explicit, that it would be aggregated and mined for what it might say about us. It takes a feat of intellectual jujitsu to construct a cognizable and actionable set of privacy interests out of the amalgamation of public activities which one transacted knowingly with a stranger in exchange for a benefit. The term privacy has become a crutch—a description of many different values of quite-different weights—that does not usefully describe the harms we fear.

The more sophisticated privacy scholars and advocates appreciate this. In his exhaustive effort to create a "Taxonomy of Privacy," Daniel Solove argues up front that "The concept of 'privacy' is far too vague to guide adjudication and lawmaking"[5] and that "it is too complicated a concept to be boiled down to a single essence." Rather, he treats privacy as "an umbrella term, referring to a wide and disparate group of related things."[6] Just how wide becomes clear over the course of his 84-page article. His taxonomy contains four principal parts, each consisting of multiple subparts—creating, all in all, a 16-part typology that ranges from blackmail to data "aggregation" and "decisional interference." And he concedes in the end that although all of the privacy harms he identifies "are related in some way, they are not related in the same way—there is no common denominator that links them all."[7] Solove's heroic effort to salvage privacy's coherence through comprehensive cataloguing has the unintended effect of revealing its unsalvagability.

[5] Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV 477, 481 (2006).
[6] *Id*. 485.
[7] *Id*. 558.

My purpose here is to propose a different vocabulary for discussing the mosaic—in some ways a simpler, cruder one, but one that both more accurately describes than privacy our behavior with respect to the mosaic and that offers more useful guidance than the concept of privacy does as to what activities we should and should not tolerate. The relevant concept is not, in my judgment, protecting some elusive positive right of user privacy but, rather, protecting a negative right—a right *against the unjustified deployment of user data in a fashion adverse to the user's interests*, a right, we might say, against databuse. The databuse conception of the user's equity in the mosaic is more modest than privacy. It doesn't ask to be "let alone." It asks, rather, for a certain protection against tangible harms as a result of a user's having entrusted elements of his or her mosaic to a third party. Sometimes, to be sure, these tangible harms will implicate privacy as traditionally understood, but sometimes, as I will explain, they will not. Think of it as a right to not have your data rise up and attack you.

Thinking about mosaic questions we currently debate in the language of privacy in terms of databuse has a clarifying effect on a number of contemporary public policy disputes. In some cases, it will tend to suggest policy outcomes roughly congruent with those suggested by a more conventional privacy analysis. In other cases, by contrast, it suggests both more and less aggressive policy interventions and market developments on behalf of users. In some areas, it argues for a complacent attitude towards data uses and acquisitions that have traditionally drawn the skeptical eye of privacy activists. Yet it also suggests more intense focus on a subset of privacy issues that are currently under-emphasized in privacy debates—specifically, issues that genuinely implicate personal security.

A Very Brief, Reductionist History of Privacy

It is not an accident that we instinctively think about the regulation of the mosaic in terms of privacy. The concept of privacy has deep roots in American democratic thought and provides a convenient vocabulary for all sorts of issues implicating personal autonomy, seclusion, reputation, and the ability to control information about oneself. It thus seems intuitive that when companies collect large quantities of data about a person or when government fishes through that person's bit stream, these actions implicate her privacy. This point is so obvious to us that we seldom stop and ask precisely what we mean by it or where the idea comes from.

Yet privacy, at least as a distinct legal concept, is a relatively recent idea, one that developed in American law and political culture only in response to the development of surveillance technologies that outmoded earlier ways of thinking about keeping government and outsiders out of one's business. This point bears emphasis: The concept of privacy only separated from the concept of property and emerged as a legal concept of its own as technologies and organizational structures rendered property rights an inadequate conceptual framework for thinking about publicity and surveillance. We created privacy, to put it simply, because we had

reached a technological tipping point that required a conceptual breakthrough.

The Constitution, which predates the separation, thus does not mention privacy explicitly. It did not need to. At the time of its drafting, it was relatively difficult to invade someone's privacy without invading his physical space. Any legal conception of privacy in that era was consequently indelibly bound up with property rights, from which it had no autonomous existence. The concern for what we later came to call privacy did, of course, exist. Indeed, it shows up in English common law long before the Founding. As early as 1604, a British court famously wrote that "the house of everyone is to him as his castle and fortress, as well for his defence against injury and violence, as for his repose."[8] Sometimes, the concern for privacy in early texts is explicit—though the word "private" tends to appear as an adjective modifying "property," not in its noun form, "privacy." Indeed, by the time of the founding of the American Republic, British courts had begun reining in the power of the King's men to raid people's houses. The celebrated cases of British Parliamentarian John Wilkes and publisher John Entick had a particularly profound impact on the later development of the Fourth Amendment.[9] And the language the British courts used in *Entick* offers a useful example of the inextricable intertwining of privacy and property in that era:

> By the laws of England, every invasion of private property, be it ever so minute, is a trespass. No man can set his foot upon my ground without my license, but he is liable to an action, though the damage be nothing. . . . Papers are the owner's goods and chattels: they are his dearest property; and are so far from enduring a seizure, that they will hardly bear an inspection; and though the eye cannot by the laws of England be guilty of a trespass, yet where private papers are removed and carried away, the secret nature of those goods will be an aggravation of the trespass, and demand more considerable damages in that respect.[10]

These cases, in other words, reflect a concern for privacy, but the concept is never separate from the broader concern about the sacrosanct nature of property. Which is cart and which is horse is never clear; they are not that distinct.

The protections in the Constitution thus surround the value that we would call privacy but they do not protect it explicitly. Similarly, as Solove's taxonomy makes clear, other values we have come to think of as contained in the notion of privacy had roots as well that long predate the emergence of privacy itself as a legal value. For example, rules against eavesdropping go back centuries.[11] The Founding generation did not attempt to embed in American law specific protections for privacy above and beyond protecting the physical spaces the individual owned and his own conscience, because it did not have to. The technology of the time

[8] Semayne's Case, (1604) Eng. Rep. 62 (K.B.).
[9] Wilkes v. Wood, (1763) 98 Eng. 489 (C.P.); Entick v. Carrington, (1765) 95 Eng. Rep. 807 (K.B.).
[10] *Entick v. Carrington*, *supra* note 9.
[11] Solove, *supra* note 5, at 492.

generally did not permit egregious invasions of privacy in the absence of some physical intrusion into someone's house, office, or things. The law of trespass and theft already kept private individuals at bay. Keeping the government out—except with cause—ensured the individual a zone of seclusion. So the Fourth Amendment, which forbids unreasonable searches and seizures, and the mostly forgotten Third Amendment, which forbids the quartering of soldiers on private property in peacetime without consent, restrained government from unwarranted invasions of the physical property of the citizen. The Fifth Amendment provided a right against self-incrimination, that is, the right to keep mum about one's own wrongdoing. And a measure of protection for the privacy of one's guilt and thought inherently resides in any right not to confess. And the First Amendment provided for freedom of religious conscience and freedom of thought and expression. But the Founders did not generalize the privacy principle that conceptually unites these restraints into something broader. Technology did not require that they do so.

The legal concept of privacy only began meaningfully to separate from the idea of property in the late 19th Century, as both technology and organizational structures evolved to permit privacy intrusions in the absence of trespass. In 1878, the Supreme Court confronted the question of whether letters entrusted to the post office required a warrant to inspect. The decision, still infused with a sense of letters as personal property, seems to hint at a broader privacy principle:

> The constitutional guaranty of the right of the people to be secure in their papers against unreasonable searches and seizures extends to their papers, thus closed against inspection, wherever they may be. Whilst in the mail, they can only be opened and examined under like warrant, issued upon similar oath or affirmation, particularly describing the thing to be seized, as is required when papers are subjected to search in one's own household. No law of Congress can place in the hands of officials connected with the postal service *any authority to invade the secrecy of letters and such sealed packages in the mail*; and all regulations adopted as to mail matter of this kind must be in subordination to the great principle embodied in the Fourth Amendment of the Constitution.[12]

A few years later, the Supreme Court all but merged the right against self-incrimination with the right against unreasonable searches and seizures—holding that the government could not compel a suspect to produce his private business papers and then use those papers against him in court. Its language—to be precise, its discussion of *Entick*—went further in invoking privacy as the relevant value at stake, though still linking it strongly to property:

> The principles laid down in [*Entick*] affect the very essence of constitutional liberty and security. They reach farther than the concrete form of the case

[12] *Ex Parte* Jackson, 96 U.S. 727, 733 (1877).

> then before the court, with its adventitious circumstances; they apply to all invasions on the part of the government and its employees of the sanctity of a man's home and the privacies of life. It is not the breaking of his doors and the rummaging of his drawers that constitutes the essence of the offence, but it is the invasion of his indefeasible right of personal security, personal liberty, and private property, where that right has never been forfeited by his conviction of some public offence—it is the invasion of this sacred right which underlies and constitutes the essence of Lord Camden's judgment. Breaking into a house and opening boxes and drawers are circumstances of aggravation, but any forcible and compulsory extortion of a man's own testimony or of his private papers to be used as evidence to convict him of crime or to forfeit his goods is within the condemnation of that judgment. In this regard, the Fourth and Fifth Amendments run almost into each other.[13]

One can see here privacy as a value beginning to assert an autonomous existence in law. But the separation from property did not become complete until technology began to permit new kinds of surveillance that required no invasion of property at all.

Anyone who doubts that the intellectual history of privacy as a legal concept is inextricably linked to the technological history of surveillance need only reflect for a moment that two of the watershed events in the development of privacy rights took place in direct response to the development of new surveillance technologies. These two events—the 1890 publication of Samuel Warren's and Louis Brandeis's seminal law review article, "The Right to Privacy," and Brandeis's subsequent dissent in the 1928 Supreme Court case of *Olmstead v. United States*—were pivotal in crafting modern American attitudes in law, policy, and culture alike towards the concept of privacy. The first responded to the invention of the instant camera and its use by the press to report on society figures. The second responded to the development of wiretapping technology.

Brandeis's first great contribution was to sever the idea of privacy from the idea of property entirely. Brandeis's and Warren's concern went far beyond the intrusion by government onto physical property belonging to an individual. For them, the issue was that

> [i]nstantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that "what is whispered in the closet shall be proclaimed from the house-tops." For years there has been a feeling that the law must afford some remedy for the unauthorized circulation of portraits of private persons; and the evil of invasion of privacy by the newspapers, long keenly felt. . . . The press is overstepping in every direction the obvious bounds of propriety and of decency. Gossip is no

[13] Boyd v. United States, 116 U.S. 616, 630 (1886).

> longer the resource of the idle and of the vicious, but has become a trade, which is pursued with industry as well as effrontery. To satisfy a prurient taste the details of sexual relations are spread broadcast in the columns of the daily papers. To occupy the indolent, column upon column is filled with idle gossip, which can only be procured by intrusion upon the domestic circle. The intensity and complexity of life, attendant upon advancing civilization, have rendered necessary some retreat from the world, and man, under the refining influence of culture, has become more sensitive to publicity, so that solitude and privacy have become more essential to the individual; but modern enterprise and invention have, through invasions upon his privacy, subjected him to mental pain and distress, far greater than could be inflicted by mere bodily injury.[14]

Brandeis and Warren here were not suggesting a constitutional right, but recognition of new common-law torts. And they made clear that protections of property were not adequate for their purposes:

> [T]he protection afforded to thoughts, sentiments, and emotions, expressed through the medium of writing or of the arts, so far as it consists in preventing publication, is merely an instance of the enforcement of the more general right of the individual to be let alone. It is like the right not be assaulted or beaten, the right not be imprisoned, the right not to be maliciously prosecuted, the right not to be defamed. In each of these rights, as indeed in all other rights recognized by the law, there inheres the quality of being owned or possessed—and (as that is the distinguishing attribute of property) there may some propriety in speaking of those rights as property. But, obviously, they bear little resemblance to what is ordinarily comprehended under that term. The principle which protects personal writings and all other personal productions, not against theft and physical appropriation, but against publication in any form, is in reality not the principle of private property, but that of an inviolate personality.[15]

For them, privacy was not defined by physical space or property but by one's ability to "retreat from the world" and avoid "publicity." A picture snapped in public and published against one's will invaded one's privacy even if it required no trespass to obtain and even if one didn't own one's own image. A newspaper article about one's affairs offended the right even if the information were all true and collected from public sources. The right to privacy in Brandeis's and Warren's conception was a right to shield one's personality from the view of others; it was bound up with personal autonomy and, as the article famously notes, "the right to

[14] Samuel D. Warren and Louis D. Brandeis, *The Right to Privacy*, 4. HARV. L. REV. 193 (1890).
[15] *Id.*

be let alone."[16]

There is a contradiction—or at least a tension—at the core of this conception of privacy, predicated as it is on the theory that property is insufficient to protect the value at stake: It necessarily claims protection as private for information *collected lawfully in public about activity conducted in public*.[17] For many years, the paradox of a privacy right concerning public acts manifested itself chiefly as a conflict between the right to privacy—which the courts began recognizing in a variety of tort claims—and the right to free speech. Brandeis's specific concerns today not only seem a bit quaint, they fly in the face of our modern understanding of the press and its function in American life. As Stewart Baker has written of Brandeis's solicitude for the privacy of Victorian society figures against media attention, "Is there anyone alive who thinks it should be illegal for the media to reveal the guest-list at a prominent socialite's dinner party or to describe how elaborate the flora arrangements were? . . . To be blunt, when he complains so bitterly about media interest in a dinner party, Brandeis sounds to modern ears like a wuss."[18]

The tension, which the courts have resolved over the years almost entirely in favor of free speech and press, was muted for decades because the volume of information in question was small. Investigating a person took time and energy, and very few people warranted that kind of attention. Not only was the amount of information available relatively slight and the number of targets relatively small, but once collected, the information had relatively few legal uses other than publication. In the absence of big databases easily mined about either individuals or society at large, it was possible to square the circle of a robust privacy interest in assorted public behaviors. Indeed, as late as 1989, the Supreme Court could hold unanimously that government "rap sheets" were shielded from disclosure under freedom of information law, though the criminal records they contained were all matters of public record, because the assembly of the information added significant value to it—value that injured privacy. The cumbersome process of compiling such material ensured a degree of "practical obscurity" that the rap sheets negated, the court found. "Plainly," the court wrote in a passage that reads today like the height of judicial naïveté, "there is a vast difference between the public records that might

---

[16] *Id.*

[17] This paradox remains a feature of the privacy literature to this day and shows up frequently. Solove, for example, writes that "Helen Nissenbaum, a professor of information technology, is quite right to argue that we often expect privacy even when in public. Not all activities are purely private in the sense that they occur in isolation and in hidden corners. When we talk in a restaurant, we do not expect to be listened to. A person may buy condoms or hemorrhoid medication in a store open to the public, but certainly expects these purchases to be private activities. Contrary to the notion that any information in public records cannot be private, there is a considerable loss of privacy by plucking inaccessible facts buried in some obscure document and broadcasting them to the world on the evening news. Privacy can be infringed even if no secrets are revealed and even if nobody is watching us." DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 44 (2004).

[18] BAKER, *supra* note 2, at 312.

be found after a diligent search of courthouse files, county archives, and local police stations throughout the country and a computerized summary located in a single clearinghouse of information."[19] Today one need not conduct a "diligent search" of anything to find out someone's criminal record, and no sane person would try to find it out with a time-consuming request to some government agency either. It's all available for sale online.[20] The world of the mosaic is not Brandeis's world. The circle is no longer squarable. We are not, to use Baker's word, wusses.

Brandeis's other great contribution to the debate over privacy and surveillance was the insistence that the Fourth Amendment offers the proper analytical frame through which to consider governmental uses of new technologies for investigative acquisition. In the context in which he reached this judgment—wiretapping—it seems today unassailable. Almost nobody, after all, now believes, as the Supreme Court held in 1928, that wiretapping is not a form of search covered by the Fourth Amendment.[21] The court at that time took a view of the amendment's coverage still conditioned by property, not privacy. There was no trespass on the individual's property in the course of tapping his phone line, and there was therefore no search, it held. As a consequence, a warrant was not required. Brandeis, in his celebrated dissent in *Olmstead*, saw things differently—that is, saw the value as privacy, not property:

> When the Fourth and Fifth Amendments were adopted, . . . [f]orce and violence were then the only means known to man by which a government could directly effect self-incrimination. [The government] could compel the individual to testify—a compulsion effected, if need be, by torture. It could secure possession of his papers and other articles incident to his private life—a seizure effected, if need be, by breaking and entry. Protection against such invasion of "the sanctities of a man's home and the privacies of life" was provided in the Fourth and Fifth Amendments by specific language. . . . But "time works changes, brings into existence new conditions and purposes." Subtler and more far-reaching means of invading privacy have become available to the government. Discovery and invention have made it possible for the government, by means far more effective than stretching upon the rack, to obtain disclosure in court of what is whispered in the closet. Moreover, "in the application of a Constitution, our contemplation cannot be only of what has been, but of what may be." The progress of science in furnishing the government with means of espionage is not likely to stop with wire tapping. Ways may some day be developed by which the

[19] Dep't of Justice v. Reporters Committee, 489 U.S. 749, 764 (1989).
[20] Numerous online sites sell criminal background data for very modest fees. See, for example, http://www.integrascan.com. Others purports to make criminal background data available for free. See, for example, http://www.criminalsearches.com.
[21] Olmstead v. United States, 277 U.S. 438, 473-74 (1928) (internal citations omitted).

> government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home. Advances in the psychic and related sciences may bring means of exploring unexpressed beliefs, thoughts and emotions. . . . Can it be that the Constitution affords no protection against such invasions of individual security?[22]

For Brandeis, the fundamental right at stake lay not in the literal words of the amendments in question—bound up as they are in physical space and, again, property. It lay in the privacy that they protected. And as new technologies became available, he insisted, that right required translation to cover the use of those technologies to keep the underlying right as real as it had been at common law under the technologies available then. While the Supreme Court took decades to adopt his vision of wiretapping, this approach ultimately prevailed not just as to bugging but also as to the larger principle. Supreme Court justices of all stripes today accept that the Fourth Amendment reaches beyond the technology of the 18th Century and requires application to today's analogous intrusions.[23]

These two foundational principles of Brandeisian, as opposed to Founding Era, privacy—that we should consider new government surveillance technologies under the rubric of the Fourth Amendment and that people have a privacy interest in activity conducted in public—have profoundly affected every aspect of our contemporary discussion of data, surveillance, and privacy. Both developed in response to technological changes and the stress they put intellectually on prior legal concepts designed to shield the individual both from government and from the outside world more generally. And both have been placed under great stress by further advances in technology.

The Conceptual Inadequacy of Privacy

Indeed, just as we once needed privacy because earlier ideas no longer described the stresses on our seclusion from the outside world, today it is privacy itself that has been outstripped by technological development. I don't mean this in some crude sense: Privacy is dead so we should stop protecting it. Property rights didn't die in the late 19th Century just because we thought up privacy, after all. Rather, the idea of property rights continued to mean more or less what it had ever meant—including some not-inconsiderable protections for privacy. The innovation of Brandeis and other thinkers was to stop relying on it for the protection of a value that, they found, it could no longer protect. Rather than go through contortions to make property rights bear weight it could not naturally bear (Do we own our personal conversations when they are traveling over phone lines? Do we

[22] *Id.*

[23] *See* Kyllo v. United States, 533 U.S. 27 (2001) (Justices Souter, Thomas, Ginsburg, and Breyer concurred in Justice Scalia's majority opinion).

own our images? Do we own our overheard thoughts and our private facts?), they created a concept that described the challenges their society faced and left property rights to protect, well, property rights. We need to do something similar—to develop a concept that describes better than does privacy the challenges posed to individuals by the mosaic. While privacy offers a comfortable vocabulary for the discussion, insofar as the word evokes a familiar set of concerns, it is ultimately an incomplete and stifling vocabulary, one that both subtly misdescribes our real concerns and behaviors and expectations with respect to mosaic data and conflates those concerns with other concerns to which they are only dimly related.

To understand this point, consider for starters the extent to which the mosaic explodes the paradox latent in the Brandeisian conception of privacy, with its claimed zone of seclusion for even public activity. This idea was one thing when we were talking about tort claims against society reporters or paparazzi. It is quite another thing now—and becomes quite unmanageable conceptually—when we are talking about a society with gargantuan and exponentially-growing quantities of data about each and every one of us. Most of this data is not plausibly protected by the Fourth Amendment.[24] Much of it is not protected by any law at all. Indeed, a great deal of the material that makes up the mosaic is not, in fact, private by any reasonable definition of the word. It is made up of *public* records, assembled and processed and made valuable and interesting through amalgamation and searchability. To insist, as some privacy advocates do, on privacy as the relevant lens for such material tends to end up pushing back against openness and transparency in government.[25]

Even the non-public records involved in the mosaic are often not quite analogous to materials we conventionally regard as private. The mosaic is not principally composed of situations quite like those in which our likenesses or our habits are gobbled up against our will by digital paparazzi and then published for the reading pleasure of a prudish Victorian society. We are, rather, willing participants in our own exposure. We give away our data at the slightest inducement with full knowledge, at least in general terms, that the companies to whom we give them will use them to market products to us. We do so in exchange for often trivial benefits—a small discount at the grocery store, a free email account, access to a news web site. Sometimes, we do it actively in explicit exchange for targeted marketing: We rate the movies that we rent and the books we buy—as well as the vendors that sell them. We wander around the web clicking that we "like" or "recommend" things and leaving public "feedback" and "comments" on other things. The society figures whose privacy evoked Brandeis's concerns were not selling their pictures to the press—and selling them extraordinarily cheaply—and then complaining about exposure. Nor would such behavior, I suspect, have triggered Brandeis's sympathy. And while privacy

[24] Under reigning Fourth Amendment doctrine, after all, material voluntarily disclosed to a third party is not protected. *See* United States v. Miller, 425 U.S. 435, 443 (1976).
[25] *See* SOLOVE, *supra* note 17, at 127-139.

advocates correctly point out that it is simply impractical to engage with the modern world without generating a huge quantity of digital fingerprints, that too reflects a mass societal judgment about the relative value of convenience and seclusion, of sharing information and hording it, of networking and privacy. We are not, to repeat, a society of wusses—which is precisely why Brandeis's and Warren's article reads today so quaintly.

In fact, in our more exuberant engagements with the mosaic, we are in a meaningful sense actively doing to ourselves the very things Brandeis feared would be done to us. The wild popularity of sites like Facebook, MySpace, and Twitter—all of which are devoted to sharing personal data with communities of various sizes—means that we are all posting our own and one another's images, comments, and thoughts. And while one might argue that such sites should protect architecturally one's ability to control to whom one says what—indeed, I would agree with this general proposition—as a practical matter, building privacy into social networking is akin to efforts to make war more humane. They are worthy and necessary, I am sure, but they are also ultimately inconsistent with the underlying project. The essence of social networking is the sharing of enough personal data to be interesting. A society that goes in big for social networking cannot simultaneously demand, as Brandeis and Warren did, too much legal solicitude for the "protection of the personal appearance, sayings, acts, and . . . personal relation, domestic or otherwise."[26] It has voted with its feet.

Yet my point, as I said earlier, is not that privacy is dead and that we should give it a proper burial or that it is irrelevant to considerations of the mosaic. To the contrary, it remains a vital value. My point, rather, is more limited: that it is not accurate empirically or, in my judgment, desirable normatively to treat it as the dominant value at stake in the individual's equities in the mosaic. Our continued reliance on the concept of privacy has a way of conflating a wide array of very different concerns and threats that are by no means of comparable severity and seriousness.

Consider for a moment the astonishing range of mosaic issues that we treat under the rubric of privacy. One of the many virtues of Solove's efforts to catalogue privacy harms is the fleshing out of this diversity. I offer the following survey, which groups the harms rather differently and less comprehensively than Solove does, not in an effort to set up a competing taxonomy but, rather, in an effort to give a high-altitude glimpse of the landscape's sweep. There is, for starters, what we might call privacy as sentiment—the way it makes us feel when information about us is available to strangers and the sense that, quite apart from any tangible damage a disclosure might do, our data is nobody else's business, particularly not government's. Privacy as sentiment is at the core of the Brandeisian conception of privacy. It is also central to writers like Rosen and Solove. Solove devotes an entire chapter of one of his books to the way "digital dossiers" make us feel like characters in Franz Kafka's *The Trial*:

[26] Brandeis and Warren, *supra* note 14.

> In the context of computer databases, Kafka's *The Trial* is the better focal point for the discourse than Big Brother. Kafka depicts an indifferent bureaucracy, where individuals are pawns, not knowing what is happening, having no say or ability to exercise meaningful control over the process. . . . *The Trial* captures the sense of helplessness, frustration, and vulnerability on experiences when a large bureaucratic organization has control over a vast dossier of details about one's life.[27]

Both writers suggest that the fact of surveillance makes people behave differently, chilling deviant behavior and encouraging conformity.

Privacy as sentiment is central in contemporary discussions of the mosaic. A recent Federal Trade Commission staff report on digital privacy, for example, notes that the commission's prior conception of privacy based on harm prevention and ensuring consumer informed consent for the use of data was inadequate because,

> for some consumers, the actual range of privacy-related harms is much wider and includes . . . the fear of being monitored or simply having private information "out there." Consumers may feel harmed when their personal information—particularly sensitive health or financial information—is collected, used, or shared without their knowledge or consent or in a manner that is contrary to their expectations.[28]

In this conception of privacy, we do not look to the specific tangible harm that a disclosure or collection does to a person. The disclosure or collection is itself the harm because of the way it makes him or her feel—and because of the behavioral change it may induce.

A good example of privacy as sentiment in contemporary public policy is the long-running dispute between the European Union and the United States over the provision of airline passenger data to American law enforcement. Europeans have objected to this on privacy grounds.[29] Yet in the voluminous literature the subject has sparked, there is very little consideration of the specific harms to airline passengers of the government's receiving the same data that these passengers give to the airlines when they make reservations for international travel. The harm seems simply to be the fact of having one's data reported at all. It is presumed, rather than argued. And it is therefore unrebuttable. Privacy as sentiment is particularly apt to lose in the public policy arena, and in the marketplace, since it pits feelings—often non-specific and always intangible and frequently not shared universally—against presumably valid and specific public goods or private

---

[27] SOLOVE, *supra note* 17, at 38.

[28] FEDERAL TRADE COMMISSION, PROTECTING CONSUMER PRIVACY IN THE INFORMATION AGE 20 (2010), http://www.ftc.gov/os/2010/12/101201privacyreport.pdf.

[29] For a good overview of the subject from the perspective of the United States government, *see* STEWART BAKER, *supra* note 2, at 89-105.

interests. In the case of passenger name records data, for example, the United States has prevailed over Europe in this battle time and again.

A related conception of privacy sees in it some kind of right against targeted advertising and behavioral profiling—at least in its more aggressive forms. The recent FTC staff report is infused throughout with this vision, a sense that consumers should "be able to choose whether to allow the collection and use of data regarding their online searching and browsing activities."[30] The report proposes "a more uniform and comprehensive consumer choice mechanism for online behavioral advertising, sometimes referred to as 'Do Not Track.' Such a universal mechanism could be accomplished by legislation or potentially through robust, enforceable self-regulation."

Many commentators also see in privacy some right to control our reputations. In a lengthy *New York Times Magazine* article last year, Rosen discussed "the costs of an age in which so much of what we say, and of what others say about us, goes into our permanent—and public—digital files. The fact that the Internet never seems to forget is threatening, at an almost existential level, our ability to control our identities; to preserve the option of reinventing ourselves and starting anew; to overcome our checkered past."[31] Solove wrote an entire book entitled *The Future of Reputation* around the thesis that: "we must protect privacy to ensure that the freedom of the Internet doesn't make us less free. But to do so, we must rethink our notions of privacy. We must also balance the protection of privacy against freedom of speech. And we must find a workable way for the law to achieve these goals."[32]

Finally, at the higher end of the harms scale, privacy concerns morph into matters of personal security. Systems that do not adequately protect user privacy give rise to identity theft, fraud, financial crimes, and stalking, after all. A lack of privacy can also expose a person, under some circumstances, to unjustified arrest and prosecution and other adverse actions at the hands of government. A great many personal-security issues associated with the mosaic ultimately boil down to questions of system integrity and identity verification—and these are matters impossible to sever from the privacy, for example, of passwords or of personal data not intended for disclosure. The security of your online bank accounts is not severable from the privacy of those accounts and the records they contain.

This very brief and far-from-comprehensive overview of the work we are asking the concept of privacy to do for us gives a flavor of its breadth and diversity. We use the word to describe everything from a non-specific set of anxieties quite divorced from any particular imagined harm to matters implicating in a tangible and specific sense most fundamental matters of personal security and safety. With all the weight we put on the concept, no wonder that it bears it badly.

---

[30] FEDERAL TRADE COMMISSION, *supra note* 28, at vii.

[31] Jeffrey Rosen, *The Web Means the End of Forgetting*, N.Y. TIMES, July 21, 2010, http://www.nytimes.com/2010/07/25/magazine/25privacy-t2.html

[32] DANIEL J. SOLOVE, THE FUTURE OF REPUTATION: GOSSIP, RUMOR, AND PRIVACY ON THE INTERNET 11 (2007).

If we use the notion of privacy to protect such a wide array of interests, we can reasonably expect it to shield none of them very effectively.

And, in fact, privacy describes rather inaptly our real expectations with respect to third-party handling of mosaic data—at least to the extent that our behaviors in the marketplace reflect our expectations. Whatever political vocabulary we apply to mosaic issues, we don't seem to operationalize an expectation of non-disclosure or confidentiality in our behavior. Indeed, when one stops and contemplates what genuinely upsets us in the marketplace, privacy does not describe it well at all. It's not just that we happily trade confidentiality and anonymity for convenience. It's that we seem to have no trouble with disclosures and uses of our data when they take place for our benefit. For example, we positively expect our credit card companies to keep an eye on our transactions to protect us against fraud. We do not experience a sense of violation when computers—and ultimately humans—mine our data for irregularities in those transactions and then call us to verify their legitimacy. We don't mind credit reporting when the details the agencies report are favorable, accurate, and enable us to obtain credit. Huge numbers of consumers happily let the contents of their emails guide the advertising they receive from their email providers. We react with equanimity when companies use our purchase data to recommend further purchases or when they amalgamate data from multiple sources to provide us with the services we want. We do not punish companies that aggressively use our data for purposes of their own, so long as those uses do not cause us adverse consequences. Were we actually concerned with the idea that another person has knowledge of these transactions—what might now be described as "privacy per se"—we would react to these, and many other, routine online actions quite hostilely. We would not knowingly allow merchants to track our purchases in exchange for a small discount. We would not move aggressively away from the anonymity of cash transactions.

Yet we have no trouble with outside entities handling, managing, and even using our data—as long as we derive some benefit or, at least, incur no harm as a result. Rather, we positively expect uses of our data that will benefit or protect us; we tolerate uses of them so long as the consequences to us are benign; and we object viscerally only where the use of our data has some adverse consequence for us. To put the matter simply, we react positively or negatively to the collection, storage, and use of our mosaic data *not in proportion to whether that data is used in a fashion that protects our privacy or confidentiality but in proportion to whether it is used for our benefit or to our detriment and critically, how seriously to our detriment*. This is not privacy we are asking for. It is something else.

I submit that what we seek in our interactions with the mosaic is some degree of protection against what we might term "databuse." Databuse is not privacy, though the two concepts clearly overlap. Think of it as the malicious, reckless, negligent, or unjustified handling, collection, or use of a person's data in a fashion adverse to that person's interests and in the absence of that person's knowing consent. Databuse can occur in corporate, government, or individual handling of

data. Our expectations against it are an assertion of a negative right, not a positive one. It is in some respects closer to the non-self-incrimination value of the Fifth Amendment than to the privacy value of the Fourth Amendment. It asks not to be left alone, only that we not be forced to be the agents of our own injury when we entrust our data to others. We are asking not necessarily that our data remain private; we are asking, rather, that they not be used as a sword against us without good reason.

Databuse and the Mosaic

Envisioning mosaic privacy as an expectation against databuse has both normative and empirical advantages over a more traditional privacy analysis. Empirically, the expectation against databuse seems to describe more precisely than does the umbrella term privacy the circumstances in which the policy process and the market end up taking seriously or dismissing claims regarding the collection, handling, and use of data. That is, it describes the directional momentum of what we term privacy policy. Loosely speaking, that is that privacy claims tend to lose when they lack a plausible assertion that the failure to protect a privacy interest will result in specific and tangible harms to individuals. Another way to think about this point is that, our rhetoric aside, we are moving away as a society from honoring claims of privacy as sentiment and towards an insistence that for a privacy claim to be cognizable as a problem warranting public policy attention, there must be some asserted harm. Confronted by a claim of a privacy invasion, modern legal culture is asking a second-order question: "Yes, but so what? What harm does it do you?" Only when the answer to that second-order question is not some faltering reiteration of an injury to sentiment does the policy process treat the claim as warranting a serious response.

Normatively, the databuse lens offers a useful means of clarifying matters we now tend to debate as privacy questions yet which often get stuck in the argumentative rut of privacy—in which a privacy claim is asserted by some and rejected by others with no obvious means of weighing an individual's expectation of an ill-defined conception of privacy against some other valid interest. That is to say that the debate is heading in the direction it is taking for a good reason—and that the direction is to be encouraged, not resisted. It leads to a simpler analytical lens through which to look at questions we now evaluate in terms of privacy impact: Instead of asking what obligation a data holder has to protect user privacy and stopping there, *we should ask instead what user harm is likely from the proposed, collection, handling and deployment of data and what obligation the third party collector should incur to prevent those harms.*

I should pause here to acknowledge an element of tautology in this formulation, because the harms to which I refer here can certainly include pure privacy harms of the type that Solove catalogues in his taxonomy. Avoiding a traditional privacy analysis in search of more-tangible user harms can thus quickly

morph back into a fairly traditional privacy analysis when those tangible user harms turn out to be privacy invasions. For example, if you store your diary on a cloud-based document storage system, like, for example, Google Docs or Dropbox, and the security of that system were to be compromised, either because of system failure or because you were careless with your password, the harm you would suffer would be the availability of your diary to people for whom it was not intended and the potential exposure of your private thoughts and the damage to your reputation that might follow from that exposure. This would be a privacy problem of a very traditional sort, but most people would nonetheless recognize it as a tangible harm.

But an approach based on avoiding databuse will not always double back and end up replicating by another name the same debate framed in terms of privacy. Indeed, it will tend to militate against claims of privacy as sentiment and will tend as well to focus attention on the space where privacy merges into larger questions of personal cybersecurity and areas where the consequences to individuals of failure to protect data from abuse can be quite dire. Sometimes, it will suggest a more tolerant attitude towards data use and collection than will a traditional privacy focus; sometimes it will suggest roughly the same degree of concern; and sometimes it will also suggest a *greater* degree of concern than privacy advocates tend to place on certain data handling matters. To illustrate this point, let us examine a few cases both from the point of view of databuse and from a stricter privacy point of view and see where they do and do not suggest similar analyses.

Consider first an area, discussed briefly above, where a harms focus proves a great deal more tolerant of collection and use of mosaic data than does a privacy analysis: the Department of Homeland Security's collection of passenger airline reservation data for international flights. The European Union's privacy-as-sentiment approach to this sort of data—an approach almost entirely detached from any actual or likely consumer harm—has made Passenger Name Record (PNR) data an ongoing point of friction between the United States and Europe on security matters. Europe has repeatedly sought to limit U.S. collection of PNR data from airlines operating under European jurisdiction; the U.S. government uses such data to look for anomalies that may suggest security problems. The EU's highly formalistic approach to privacy, supported by many domestic privacy groups, has bewildered American officials, who have noted that the data are not especially sensitive and generally include material—passport numbers, for example—of which the government will learn anyway when the traveler presents at a port of entry. Indeed, it is hard to identify any concrete harms that accrue to anyone as a result of government collection and analysis of data that travelers to the United States willingly provide to airlines. The tangible harms the policy debate does identify—the possibility of data leakage, for example, or the misuse of data, or its use to engage in ethnic profiling, are all addressable by means well short of eschewing collection generally or encumbering it arbitrarily. The strict privacy analysis, in short, sees a grand harm in the fact of the programmatic collection itself and does not concern itself with whether that programmatic

collection yields actual harms to individuals, nor does it take much comfort in the amelioration of those harms. By contrast, a databuse analysis would yield a very different approach. It would largely avoid the question of whether the fact of collection affects some grand conceptual privacy violation and focus *only* on the question of tangible harms and their amelioration. The harms being hard to identify here and relatively easy to address, a databuse focus would not yield a great deal of concern about such a program.

This is not a singular example. A great many privacy controversies fade, or change, if one focuses not on the fact of mosaic data's collection, use, or disclosure per se but on identifying, preventing or ameliorating databuse. In particular, government mining of large data sets—like, for example, the records of money flows kept by the banking consortium SWIFT—looks suddenly less threatening. After all, nobody is prevented from moving money because the program makes transfer data available to the Treasury Department. Nobody even suffers adverse legal consequences as a result of engaging in a pattern of transactions that catches the eye of intelligence officials. The only consequence of such a pattern—assuming the transactions themselves are legal—is that a person may receive closer investigative scrutiny. While government data-mining horrifies privacy advocates, a databuse analysis suggests a certain degree of equanimity about it, at least with respect to the fact of a data-mining program itself. It would, however, raise certain questions about the manner in which such a program is conducted. Are there protections against the malicious use of the data in question? How rigorously is access to them controlled and audited? More generally, is the system maintained and operated in a fashion that minimizes the risks of harms of various types?

A databuse focus gives rise to a similar analysis of behavioral and targeted advertising—which are really a kind of private sector analogue to government data-mining programs.

Behavioral advertising upsets privacy advocates for a variety of reasons, a mixture of privacy as sentiment, concern about harms to individuals, and concern about data collection under false pretenses. A databuse focus here would substantially narrow the range of anxiety. The fact of using someone's data to market products to that person does not in-and-of-itself do the person any damage. Matching consumers to products they wish to buy is a service, not a harm, after all. And we are not such automatons that we are unable to avoid buying things that marketers send our way. What's more, the notion that companies that give us some benefit in exchange for our data must then refrain from using that data to sell things to us because of the way it makes us feel seems insubstantial—a demand to reap the benefits of a transaction without paying the costs of it. If one doesn't want people using data to market products, one should not give one's data away to marketers.

What does not seem insubstantial, however, is the concern about deceptive data practices, tracking by third party marketers to whom the user might never knowingly have given data, insecure systems, and the failure to correct data errors.

These, after all, can lead to specific user harms: denied credit, identity theft, and the not-truly-consensual or ill-informed disclosure of data, for example. A person who has been mislead into giving up data he would not otherwise have given up has been cheated into a transaction in which he was not a willing participant. And insecure systems heighten people's risk of identity theft and other very tangible harms. So while a databuse analysis does not give rise to great anxiety about the fact of behavioral advertising itself, it does suggest a certain insistence that companies be clear and straightforward about their practices and responsible and secure custodians of people's data. In all of these cases, a databuse focus will tend to tolerate greater collection and use of data than will a privacy analysis but will insist that use be responsible and neither malicious nor fraudulent.

Next, let us consider an issue of some contemporary moment in which a databuse focus will tend to yield a similar analysis to a privacy focus: the disclosure of email contents stored in the cloud pursuant to subpoena instead of, as many civil libertarians and businesses prefer, pursuant only to warrant issued on a showing of probable cause.[33] Currently, the government can obtain stored email communications with a mere subpoena provided either that the email is more than 180 days old or that it has been accessed by the end user. If neither of these conditions has been met, the contents of the email can be accessed only with a search warrant.[34] For the past several years, a coalition of civil liberties and business groups has been trying to heighten the protection for stored email. The language of the dispute is privacy. But a harms-prevention analysis will, in my view, tend to produce a congruent analysis.

The harms associated with the disclosure of personal communications to law enforcement, after all, are pretty easy to identify. The person whose personal email is turned over to law enforcement yet against whom law enforcement has no probable cause of a crime (the standard for a warrant) but merely because the information is relevant to a grand jury investigation (the standard for a subpoena) has disclosed to law enforcement all manner of personal material. This may reveal improprieties previously unknown to law enforcement. It may reveal severely embarrassing but legal conduct that may end up publicly disclosed in court proceedings. And yes, it may bring about pure privacy harms, an exposure of that

---

[33] For background on this subject, see Orin S. Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, 62 STAN. L. REV. 1005, 1007-1008 (2010); J. BECKWITH BURR, THE ELECTRONIC COMMUNICATIONS PRIVACY ACT OF 1986: PRINCIPLES FOR REFORM (2010), *available at* http://www.digitaldueprocess.org/files/DDP_Burr_Memo.pdf (last visited on Dec. 20, 2010); *See* BENJAMIN WITTES, WELLS C. BENNETT & RABEA BENHALIM, RATIONALIZING GOVERNMENT COLLECTION AUTHORITIES: A PROPOSAL FOR RADICAL SIMPLIFICATION (2011), http://www.brookings.edu/topics/justice-and-law.aspx; United States v. Warshak, 631 F.3d 266 (6th Cir. 2010).

[34] 18 U.S.C. § 2703(a)-(b) (West 2011) (requiring government to obtain a warrant before collecting the contents of un-accessed "in electronic storage in an electronic communications system for one hundred and eighty days or less" but allowing collection of contents of older communications, and the contents of accessed communications stored in remote computing services, with a subpoena).

person's private affairs to individuals or a public with which he or she does not wish to share it. These harms are both tangible and potentially significant. And while this fact does not answer the question of the standard under which the government should be able to access such data, it is a weighty consideration on the side of restricting access whether one considers the matter under the rubric of privacy or under the rubric of databuse. Interestingly, the coalition gathering around enhancing protection for stored email may well ultimately prevail—either legislatively or in the courts. Where privacy claims are backed up with tangible claims of real harm, privacy does not necessarily lose.

Finally, a focus on harms would counsel much *greater* policy attention to certain mosaic data issues than does a traditional privacy analysis. Specifically, a harms focus would give a higher salience to the many identity-authentication and personal-security issues raised by the mosaic—the threats of identity theft and stalking that have grown up alongside the mosaic, for example. These issues are strangely undervalued in privacy advocacy. The Web site of the Electronic Privacy Information Center, for example, has sections for "hot policy issues"—which include "body scanners," "cloud computing," "Iraqi biometric ID system," "social networking privacy," "national ID," and "smart grid." EPIC does not include issues like identity theft.[35] Run a search on the term "identity theft" on the Web site of the Center for Democracy and Technology, and only scattered references arise. The site has a section devoted to "spyware"—the most recent entry under which dates from 2008.[36] And a section devoted to "identity management" is chiefly concerned with the privacy impact of identity authentication schemes, not the privacy impact of the activities that necessitate those schemes.[37] When privacy advocates discuss personal security matters, they often do so as a kind of afterthought. In his book, *The Digital Person*, Solove's discussion of identity theft is brief and buried in the sixth chapter; it appears only after far lengthier discussions of the dehumanizing effects of "digital dossiers."[38] While Solove terms identity theft "a privacy problem that resembles a Kafkaesque nightmare," it isn't the core privacy problem with which he concerns himself. For many people, the personal security issues associated with the mosaic seem somehow outside of the realm of real privacy altogether.

A focus on databuse would place a great deal more emphasis on such issues—indeed, would treat them as the data handling matters of the greatest concern both to society at large and to the average user. It would seek to maximize the individual's right to leave tiles all over the mosaic without incurring undue risk to himself in the course of doing so. It would merge a conception of privacy with a

---

[35] ELECTRONIC INFORMATION PRIVACY CENTER, http://epic.org/ (last visited Feb. 14, 2011).

[36] *Spyware*, CENTER FOR DEMOCRACY AND TECHNOLOGY, http://www.cdt.org/issue/spyware (last visited Feb. 14, 2011).

[37] *Identity Management*, CENTER FOR DEMOCRACY AND TECHNOLOGY, http://www.cdt.org/issue/identity-management (last visited Feb. 14, 2011).

[38] SOLOVE, *supra* note 17, at 1.

conception of personal security—for the two are far more linked than people intuitively think. If one's communications are not secure, they are not private either, and if they are not private, they not secure. If one's passwords are not private, one's bank accounts are not secure. To lay the matter bare, for most consumers, increasing the security of their mosaics *is synonymous with increasing its privacy*. For that reason, I suspect that focusing on the prevention of the tangible harms associated with databuse—one which treats the emotional aspects of privacy as collateral—will nonetheless do more to protect the emotional aspects of privacy than a policy focus on those aspects ever could. Personal security represents an area where privacy will not lose in the public policy space, and a great deal of privacy as sentiment can win protection if it comes along for the ride.

Conclusion

We debate mosaic issues in the language of privacy because privacy is the only word we've got. It is not, however, the value we are implementing in fact as a society or the value that we really expect as individuals from the companies and governments with which we interact. That value is something else—something that lacks a name in common parlance but amounts to an expectation against hostile, deceptive, or negligent use and handling of data we entrust to third parties. It is an expectation that our data will work for us, not against us, and that while our interests won't always be congruent with those who hold the tiles of our mosaics, the custodians of our tiles owe us consideration—at least to do us no harm.

This is not privacy. It is something else. The sooner we accept that in discussing these issues, we are not operating inside of Brandeis's privacy framework but, rather, engaging in the very project he undertook—that is, imagining new legal categories for new surveillance challenges wrought by technology—the sooner we will confront them effectively and in a fashion that satisfies the many competing interests at stake in the mosaic.

Author

Benjamin Wittes is a senior fellow in Governance Studies at The Brookings Institution. He is the author of *Detention and Denial: The Case for Candor After Guantanamo*, forthcoming from the Brookings Institution Press. He is also the author of *Law and the Long War: The Future of Justice in the Age of Terror*, published in June 2008 by The Penguin Press, and the editor of the 2009 Brookings book, *Legislating the War on Terror: An Agenda for Reform*. He co-founded and co-writes the *Lawfare* blog (http://www.lawfareblog.com/), which is devoted to non-ideological discussion of the "Hard National Security Choices," and is a member of the Hoover Institution Task Force on National Security and Law.

Governance Studies
The Brookings Institution
1775 Massachusetts Ave., NW
Washington, DC 20036
Tel: 202.797.6090
Fax: 202.797.6144
www.brookings.edu/governance.aspx

Editor
Christine Jacobs

Production & Layout
John S Seo

E-mail your comments to gscomments@brookings.edu