Privacy-Privacy Tradeoffs

David E. Pozen*

Legal and policy debates about privacy revolve around conflicts between privacy and other goods. But privacy also conflicts with itself. Whenever securing privacy on one margin compromises privacy on another margin, a privacy-privacy tradeoff arises.

This Essay introduces the phenomenon of privacy-privacy tradeoffs, with particular attention to their role in National Security Agency (NSA) surveillance. After explaining why these tradeoffs are pervasive in modern society and developing a typology, the Essay shows that many of the arguments made by the NSA’s defenders appeal not only to a national security need but also to a privacy-privacy tradeoff. An appreciation of these tradeoffs, the Essay contends, can illuminate both the structure and the stakes of debates over surveillance law specifically and privacy policy generally.

INTRODUCTION

Privacy clashes with important social values. We are told as much all the time.1 Commentators struggle to reconcile privacy and security,2 privacy and efficiency,3 privacy and technological innovation,4 and privacy and free speech,5 among other (real or imagined) antinomies.6 Privacy is constantly being juxtaposed with competing goods and interests, balanced against alternative needs and demands. Legal and policy debates about privacy revolve around these tradeoffs.

But privacy also clashes with itself. That is to say, in many social and regulatory contexts, enhancing or preserving privacy along a certain dimension may entail compromising privacy along another dimension. If they wish to be more analytically rigorous, theorists and decisionmakers must take such privacy-privacy tradeoffs into

---

1 See Julie E. Cohen, Configuring the Networked Self 148 (Yale 2012) (“The mainstream public debate about privacy typically portrays privacy as a good infinitely amenable to being traded off against other goods.”). See also Colin J. Bennett and Charles D. Raab, The Governance of Privacy 23 (MIT 2006) (“The [dominant] privacy paradigm, based on a conceptualization of distinct private and public realms, almost inevitably leads the debate to a discussion of how privacy conflicts with social or community values . . . .”).

2 See Helen Nissenbaum, Privacy in Context 108 (Stanford 2010) (“One of the most frequently cited conflicts . . . is between privacy and security.”).

3 See id at 109 (“[P]rivacy is regularly challenged by a desire or need for greater efficiency.”).

4 See, for example, Stewart Baker, Skating on Stilts 313–15 (Hoover 2010).

5 See, for example, Eugene Volokh, Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People from Speaking About You, 52 Stan L Rev 1049 (2000).

6 For a particularly intriguing supplement to the standard list, see Lior Jacob Strahilevitz, Privacy Versus Antidiscrimination, 75 U Chi L Rev 363 (2008).
account. If they wish to advance the cause of privacy, civil libertarians must do the same.

Privacy-privacy tradeoffs come in a variety of flavors. Sometimes they are advertised as such. The Transportation Security Administration’s PreCheck program invites travelers to “volunteer personal information in advance” if they wish “to leave on their shoes, belts and light outerwear and keep their laptops in their bags.” More often, privacy-privacy tradeoffs simply follow from scarce resources and opportunity costs. A tenant on a fixed budget who spends money soundproofing her walls will have less to spend on mending her window curtains or protecting her online identity. Other times, these tradeoffs may be caused by behavioral responses and dynamic feedback effects. Increasing airline-passenger privacy levels from \( X \) at Time 1 to a multiple of \( X \) at Time 2 may increase the odds of a terrorist attack, with the consequence that passengers’ privacy levels will be reduced to a fraction of \( X \) at Time 3. In still other cases, risk may be redistributed across different aspects or bearers of privacy. By stripping its analysts of “any privacy or anonymity when they look at [collected] data,” an intelligence agency may deter them from exceeding their investigative mandates and thereby secure a measure of privacy for the rest of society—or at least for the analysts’ love interests.

While the idea of privacy-privacy tradeoffs appears to be new to the legal literature, the basic logic behind the idea is not. Scholars in law and other disciplines have begun to explore security-security tradeoffs, liberty-liberty tradeoffs, health-health tradeoffs, democracy-democracy tradeoffs, and other...
such “internal” oppositions. Like security, liberty, health, and democracy, privacy is a complex normative value embedded in a range of complex social practices; the possibilities for conflict within such a matrix are vast. Moreover, privacy-privacy tradeoffs are not only widespread in modern society but also proliferating, as new technologies and new conceptions of privacy continually generate new ways in which privacy interests may be violated or vindicated.

This Essay introduces the phenomenon of privacy-privacy tradeoffs, along with some conceptual tools to help negotiate them. In keeping with the theme of this symposium, the Essay focuses on governmental threats to privacy and in particular on national security surveillance. It also begins to sketch links between this subject and questions of institutional design within the regulatory state. An appreciation of privacy-privacy tradeoffs, the Essay tries to show, can clarify and enrich debates over National Security Agency (NSA) surveillance specifically as well as debates over privacy policy generally.

I. PLURALISTIC PRIVACY

Before turning to the subject of tradeoffs, I need to say a few words on the subject of privacy. Setting forth a crisp definition of the latter turns out to be remarkably difficult to do. In contemporary discourse, privacy has become associated with “freedom of thought, control over one’s body, solitude in one’s home, control over personal information, freedom from surveillance, protection of one’s reputation, and protection from searches and interrogations,” among other things.\textsuperscript{15} It is a commonplace in the privacy literature to bemoan the “bewildering variety of meanings” the concept has accumulated.\textsuperscript{16} About the only “point on which there seems to be near-unanimous agreement,” Professor Helen Nissenbaum observes, “is that privacy is a messy and complex subject.”\textsuperscript{17}

In recent years, many privacy theorists have made what we might call a pluralistic turn: rejecting approaches to privacy that strive to identify its essence or its core characteristics and settling, instead, “on an understanding of privacy as an

\textsuperscript{14} See, for example, Robert E. Goodin, \textit{Global Democracy: In the Beginning}, 2 Intl Theory 175, 179 n 11 (2010).

\textsuperscript{15} Daniel J. Solove, \textit{Understanding Privacy} 1 (Harvard 2008).

\textsuperscript{16} Neil Richards, \textit{Intellectual Privacy} 8 (Oxford 2015). See also, for example, Robert C. Post, \textit{Three Concepts of Privacy}, 89 Georgetown L. J 2087, 2087 (2001) (“Privacy is a value so complex, so entangled in competing and contradictory dimensions, so engorged with various and distinct meanings, that I sometimes despair whether it can be usefully addressed at all.”).

\textsuperscript{17} Nissenbaum, \textit{Privacy in Context} at 67 (cited in note 2). Notwithstanding these laments, the “reductionist” position—which maintains that ostensible privacy claims are reducible to other sorts of claims and would be more fruitfully analyzed in non-privacy terms—has largely lost out in academic as well as popular commentary. See Judith DeCew, \textit{Privacy} (Stanford Encyclopedia of Philosophy 2013), online at http://plato.stanford.edu/entries/privacy (explaining that, against the reductionists, “most theorists take the view that privacy is a meaningful and valuable concept”).
umbrella term that encompasses a variety of related meanings.”

The concept of privacy, on this view, comprises a web of overlapping conceptions, dimensions, and values, none of which necessarily has lexical priority over any other. Professor Daniel Solove’s work is exemplary in this regard. Drawing on Ludwig Wittgenstein’s notion of family resemblances, Solove forcefully argues against conceptualizing privacy through a priori generalizations, such as necessary and sufficient conditions, in favor of a “pluralistic,” “bottom up” approach focused on “privacy problems.”

Reviewing the extensive treatments of privacy in legal scholarship and judicial opinions, Solove finds that at least six different understandings of privacy have emerged: (1) “the right to be let alone,” (2) “limited access to the self,” (3) “secrecy,” (4) “control over personal information,” (5) “personhood,” or “the protection of one’s personality, individuality, and dignity,” and (6) “intimacy,” or “control over . . . one’s intimate relationships or aspects of life.” Solove might have added still more items to the list. Professor Kendall Thomas, for instance, has discerned “zonal, relational, and decisional” paradigms of privacy in the Supreme Court case law, focused respectively on preserving “space[s] of civil sanctuary,” “freedom to associate with others in intimate relation,” and autonomous decisionmaking on certain important matters. Professor Julie Cohen has recently urged that privacy be reimagined, in “postliberal” terms, as a resource for the development of critical subjectivity and “an interest in breathing room to engage in socially situated processes of boundary management.”

In an effort to bring some analytic order to this sprawl, Solove has developed a taxonomy of widely recognized privacy violations. It is worth reproducing the taxonomy in full:

1. Information collection
   Surveillance
   Interrogation
2. Information processing
   Aggregation
   Identification
   Insecurity
   Secondary use
   Exclusion

---

18 Richards, Intellectual Privacy at 9 (cited in note 16). Cf DeCew, Privacy (cited in note 17) (discussing theorists who “defend the view that privacy has broad scope, inclusive of the multiple types of privacy issues described by the [U.S. Supreme] Court, even though there is no simple definition”).
19 Solove, Understanding Privacy at 8–9, 39–77 (cited in note 15).
20 Id at 12–37.
22 Cohen, Configuring the Networked Self at 149 (cited in note 1).
3. Information dissemination
   Breach of confidentiality
   Disclosure
   Exposure
   Increased accessibility
   Blackmail
   Appropriation
   Distortion

4. Invasion
   Intrusion
   Decisional interference

For purposes of this Essay, it does not much matter whether these classifications are compelling in all particulars, or whether the messiness and complexity of privacy will ever be satisfactorily resolved. The important thing to see is how many interests and concerns are now taken to be privacy interests and concerns. Solove, to reiterate, has identified no fewer than six broad conceptions of privacy and sixteen broad categories of privacy problems “that have achieved a significant degree of social recognition.” This capaciousness exacerbates the dilemma of privacy-privacy tradeoffs. The more sorts of privacy claims there are, the greater the risk that there will be conflicts among them.

Just consider the first two categories in Solove’s taxonomy, surveillance and interrogation. Each activity, Solove explains, may cause privacy harms. But it does not follow that the privacy harms they cause will always or typically be additive. Surveillance and interrogation are both techniques used by law enforcement officials to gather information that may be relevant for identifying and punishing criminals. A police force that devotes significant resources to surveillance will have fewer resources left over—and perhaps less of a practical need—for interrogation. As privacy problems, surveillance and interrogation are plausible substitutes. Tightening the rules on criminal interrogation, consequently, could lead to a net decrease in a community’s privacy insofar as it pushes the police to intensify surveillance.

Or consider disclosure and blackmail. Again, each is a widely recognized menace to privacy. Yet blackmail, as Solove defines it, is nothing more or less than the threat of disclosure of truthful personal information. And that threat has no force once a given datum has become public. Voluntary divulgences about one’s personal life can be self-protective in this way. Such divulgences are a defining feature of our digital

---

23 Solove, Understanding Privacy at 10–11 (cited in note 15). See also id at 101–70 (elaborating this taxonomy).
24 Id at 102.
25 Cf Charles R. Beitz and Robert E. Goodin, Introduction: Basic Rights and Beyond, in Charles R. Beitz and Robert E. Goodin, eds, Global Basic Rights 1, 23 (Oxford 2009) (“The more rights there are, the greater the danger that we will face ‘rights-rights trade-offs’ . . . .”).
26 Solove, Understanding Privacy at 105 (cited in note 15).
The rise of what Professor Bernard Harcourt calls the “expository society”—in which people eagerly give up their most intimate details “in a mad frenzy” of “texts, Tweets, emoticons and Instagrams, e-mails and Snapchats, Facebook posts, links, shares and likes” has had at least one happy side effect for our collective privacy, in that it has rendered various forms of blackmail otiose.

Other privacy-privacy tradeoffs will be more complex, but these examples suffice to make the point. Solove offers his taxonomy to “enable courts and policymakers to better balance privacy against countervailing interests.” The very breadth of the taxonomy underscores the need to start balancing privacy against itself.

II. TRADEOFF TYPES AND TRIGGERS

When exactly does this need arise, though? And what might these balancing efforts look like? Although a comprehensive answer is well beyond the scope of this Essay, drawing some distinctions among privacy-privacy tradeoffs can help to illuminate the structure of the problem.

Governmental entities and corporations maintain countless policies that have implications for privacy. A decision to change, or not to change, any given policy can occasion at least four basic types of privacy-privacy tradeoffs. These types are not mutually exclusive and may appear in combination. The tradeoffs themselves may be intentional or inadvertent, highly visible or largely unseen.

First, a policy may shift privacy burdens or benefits from one group in the population to another. If the New York City Police Department instructs agents to stop infiltrating mosques and start hanging out at Occupy Wall Street rallies, Muslim New Yorkers may experience a gain in privacy while economic-justice crusaders experience a loss. Privacy risk can be shifted across groups that threaten harm to a certain privacy interest as well as groups that suffer the harm. An e-reader such as

---


28 To take just one recurring case, facilitating public access to records held in government databases might reduce the privacy problem of “exclusion” while increasing the risk that personal information will be disclosed or exposed to others. Cf Daniel J. Solove, The Digital Person 150–54 (NYU 2004) (discussing potential tensions between privacy and open-records laws).

29 Solove, Understanding Privacy at 10 (cited in note 15).


31 Governmental decisions are, again, the focus of this Essay, although privacy-privacy tradeoffs commonly arise from individual and corporate decisions as well.

---
Amazon’s Kindle prevents my fellow riders on the subway from seeing what I am reading, but it tells Amazon in great detail about what I am reading, including how many seconds I have spent on each page.\textsuperscript{32} We can call these sorts of privacy-privacy tradeoffs \textit{distributional tradeoffs}.

Second, a policy may shift privacy risk across time periods. This is part of the privacy bargain offered by programs such as PreCheck that do intensive vetting of prospective passengers, customers, employees, or the like at a threshold stage, on the promise of reduced scrutiny thereafter.\textsuperscript{33} Maximalist privacy policies, as suggested in the Introduction, may lead to unintended intertemporal transfers (and prove self-defeating) inasmuch as they invite bad outcomes which then generate demand for new policies that substantially slash privacy.\textsuperscript{34} We can call these sorts of tradeoffs \textit{dynamic tradeoffs}.

Third, a policy may shift risk across different privacy interests. Recall the six broad conceptions of privacy and sixteen broad categories of “privacy problems” that Solove has identified.\textsuperscript{35} Whenever a policy enhances privacy on one of these dimensions while eroding it on another, a tradeoff arises. Although the military’s Don’t Ask, Don’t Tell policy allowed gay and lesbian servicemembers to conceal information about their intimate lives, it arguably undermined other aspects of their privacy by spotlighting the question of sexual orientation and constricting their ability to control their social identities.\textsuperscript{36} Although a policy requiring that police officers wear body cameras may advance various privacy goals through averted police misconduct—for instance, by reducing the number of unreasonable searches or seizures—those same cameras raise privacy concerns for the suspects, victims,

\textsuperscript{32} Richards, \textit{Intellectual Privacy} at 128–29 (cited in note 16). Wittes and Liu emphasize, more generally, that digital technologies “we commonly think of as privacy-eroding may, in fact, enhance privacy from the people in our immediate surroundings,” even as they erode privacy vis-à-vis “large physically remote entities” such as corporations and governments. Wittes and Liu, \textit{The Privacy Paradox} at 10 (cited in note 10). Cf Orin S. Kerr, \textit{An Equilibrium-Adjustment Theory of the Fourth Amendment}, 125 Harv L Rev 476, 512–17 (2011) (noting that emerging technologies may enable new modes of surveillance while allowing for the circumvention of others).

\textsuperscript{33} See text accompanying note 7 (describing PreCheck). PreCheck also trades off different privacy interests (roughly, personal information for physical intrusion).

\textsuperscript{34} See text accompanying notes 7–8 (considering airline privacy levels). Private efforts to preserve privacy can likewise have unintended dynamic effects. In the area of surveillance, for example, a person’s use of encryption may shield her data from the immediate gaze of the intelligence services but flag her as a suspicious type, deserving of future scrutiny. See Mathew J. Schwartz, \textit{Want NSA Attention? Use Encrypted Communications} (InformationWeek, June 21, 2013), http://www.darkreading.com/risk-management/want-nsa-attention-use-encrypted-communications/d/d-id/1110475?.

\textsuperscript{35} See text accompanying notes 20–23.

\textsuperscript{36} See Kenji Yoshino, \textit{Assimilationist Bias in Equal Protection: The Visibility Presumption and the Case of “Don’t Ask, Don’t Tell,”} 108 Yale L J 485, 544–57 (1998). Cf text accompanying notes 20–22 (noting the existence of decisional, dignitarian, and relational, as well as secrecy-centered, conceptions of privacy).
bystanders, and officers who may be captured on film. Targeting one privacy risk creates a new, countervailing risk. We can call these sorts of tradeoffs (somewhat awkwardly) *dimensional tradeoffs*.

Finally, when the traded-off risks seem not just factually but qualitatively distinct from or even incommensurate with each other, we might say that a dimensional tradeoff rises to the level of a *domain tradeoff*. The privacy interests on either side of the ledger, in such a case, seem to implicate different domains of value. They “cannot be aligned along a single metric without doing violence to our considered judgments about how these [interests] are best characterized.” Perhaps the privacy problems caused by surveillance and interrogation are immiscible in this way.

It would be possible, of course, to slice privacy-privacy tradeoffs more finely. Each of these four categories might be further sorted on the basis of the number of persons affected, the probability of privacy gains or losses, or the expected magnitude or character of those gains and losses. Be that as it may, I believe the categories outlined above capture some core structural differences among privacy-privacy tradeoffs and so supply a useful if limited toolkit for analyzing this heterogeneous phenomenon.

Privacy-privacy tradeoffs might also be parsed, in more functional terms, according to the triggers or mechanisms that explain their existence. Some interventions to safeguard one form of privacy will jeopardize another form quite directly when implemented, as in the case of police body cameras. Other interventions will give rise to tradeoffs more indirectly, through the adaptive behavior they induce. Regulators or regulated parties may respond to a new measure by shifting to different practices that impinge on privacy in different ways. Vulnerable actors may overestimate a measure’s benefits and be lulled into reducing their own precautions. Strategic actors may exploit the rigidities caused by privacy

---


38 Cass R. Sunstein, *Incommensurability and Valuation in Law*, 92 Mich L Rev 779, 796, 798 (1994) (defining incommensurability in a “very thin,” or weak, sense). The possibility that privacy encompasses distinct domains of value brings us back to debates over the concept’s utility and coherence. Wherever one stands on those debates, however, it seems to me that a descriptively and phenomenologically accurate typology—one that captures how privacy is understood and experienced in contemporary society—must admit these tradeoffs.


40 See text accompanying notes 25–26 (giving the hypothetical example of a police force ramping up surveillance in response to new restrictions on interrogation).

41 See Rascoff and Revesz, 69 U Chi L Rev at 1777–78 (cited in note 39) (discussing “lulling effects”).
protections in ways that render them unsustainable. Policymakers may also bring about or exacerbate privacy-privacy tradeoffs through ignorance of relevant facts or future contingencies; through analytic error, including selective attention to a certain aspect of privacy to the neglect of others; or through the standard opportunity costs associated with devoting limited resources to any particular concern.

The foregoing points can be distilled into a simple schematic. Although just one of many possible ways to carve up the landscape, this typology furnishes a serviceable conceptual map and gives a sense of the regularity, as well as the endless variety and fluidity, of privacy-privacy tradeoffs.

### TABLE 1. A TYPOLOGY OF PRIVACY-PRIVACY TRADEOFFS

<table>
<thead>
<tr>
<th>Tradeoff Type</th>
<th>Traded-Off Element</th>
<th>Trigger</th>
</tr>
</thead>
<tbody>
<tr>
<td>Distribution</td>
<td>Social groups</td>
<td>Changed circumstances</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Direct (side) effects</td>
</tr>
<tr>
<td>Dynamic</td>
<td>Time periods</td>
<td>Error</td>
</tr>
<tr>
<td>Dimensional</td>
<td>Privacy interests</td>
<td>Feedback effects</td>
</tr>
<tr>
<td>Domain</td>
<td>Qualitatively distinct privacy</td>
<td>Ignorance</td>
</tr>
<tr>
<td></td>
<td>interests</td>
<td>Lulling effects</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Opportunity costs</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Substitution effects</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Etc.</td>
</tr>
</tbody>
</table>

### III. PRIVACY-PRIVACY TRADEOFFS AND NSA SURVEILLANCE

We are now in a position to see more clearly both the structure and the stakes of current debates over NSA surveillance reform. As this Part will show, many of the justifications offered by the NSA’s defenders appeal not only to a national security need but also to a privacy-privacy tradeoff. These arguments may not be good arguments; their force depends on the practical realities of surveillance as well as one’s normative views about which forms of privacy matter most. But the arguments

---

42 See text accompanying notes 7–8 (noting possible iterated interactions between airline-passerger privacy levels and terrorist threats).
43 See generally Robert K. Merton, *The Unanticipated Consequences of Purposive Social Action*, 1 Am Sociological Rev 894, 898–902 (1936) (identifying ignorance, error, and “the imperious immediacy of interest” as pervasive causes of unintended consequences). Cf id at 901 (discussing errors “where the actor attends to only one or some of the pertinent aspects of the situation which influence the outcome of the action”); Stephen Holmes and Cass R. Sunstein, *The Cost of Rights* 125 (Norton 1999) (explaining that “the problem of selective attention” can both generate and obscure rights-rights and risk-risk tradeoffs).
cannot be fairly assessed—or compellingly countered—without an understanding of the privacy-privacy tradeoffs on which they are premised.

A. NSA Analysts vs. Ordinary Citizens?

We have already touched on one such argument: the contention that by minimizing the network privacy of its own employees and contractors, the NSA can safeguard the communications privacy of everyone else. Former NSA General Counsel Stewart Baker has proposed that this tradeoff be made the centerpiece of any new reforms. In Baker’s own words:

The short answer is that we should protect privacy . . . by working with technology, not against it. In particular, we can use information technology to make sure that government officials lose their privacy when they misuse data that has been gathered for legitimate reasons. Information technology now makes it easier to track every database search made by every user, and then to follow any distribution of that data outside the system.

The attraction of this proposal, apart from the vision of using technology to tame technology, lies in its promise of a stark distributional tradeoff. NSA analysts’ privacy losses will be We the People’s gains. As redistributive schemes go, this one is about as unobjectionable as it gets. Not only do ordinary citizens outnumber NSA analysts by many orders of magnitude, but the latter’s privacy interests in being given unfettered access to the former’s data seem tenuous at best.

The major limitation of this proposal is that it is unclear how much privacy would actually be redistributed. Baker seeks to detect and deter the “misuse” of collected data, such as unlawful disclosures to the media or prurient snooping for personal rather than professional reasons. The privacy problems raised by such misuse, however, are just a subset of the privacy problems raised by NSA surveillance, and not necessarily the most concerning subset. Even if implemented to a T, Baker’s proposal would only enhance ordinary citizens’ privacy with respect to the rogue behaviors of individual NSA analysts; as a distributional tradeoff the proposal seems stark, but as a dimensional tradeoff it is quite limited. Although this

44 See text accompanying notes 8–9.
45 Baker, Skating on Stilts at 321 (cited in note 4). See also id at 340–41 (expanding on this idea); The Administration’s Use of FISA Authorities, Hearing Before the House Judiciary Committee, 113th Cong, 1st Sess 75 (2013) (statement of Stewart A. Baker) (“FISA Hearing”) (contending that the “best way” to protect privacy is for “the government to use new technologies to better monitor government employees who have access to sensitive information”); Nathan Alexander Sales, Domesticating Programmatic Surveillance: Some Thoughts on the NSA Controversy, 10 I/S: J L & Pol Info Socy 523, 540–41 (2014) (arguing that “programmatic surveillance systems should have technological safeguards that protect privacy and civil liberties by restricting access to sensitive information and tracking what officials do with it”).
may be a trade worth making, it is not responsive to many of the privacy concerns animating the reform movement.

B. Cybersecurity vs. Cybersurveillance?

Baker’s argument envisions the NSA as the guardian of Americans’ privacy vis-à-vis internal threats posed by its own (badly behaving) employees. Another prominent argument envisions the NSA as the guardian of Americans’ privacy vis-à-vis external threats to cybersecurity. “To keep our computer and telecommunications networks secure,” Professor Jack Goldsmith contends, “the government will eventually need to monitor and collect intelligence on those networks using techniques similar to ones [many liberals] find reprehensible when done for counterterrorism ends.”46 Specifically, the Federal Bureau of Investigation’s General Counsel has suggested, “the government needs to be able to monitor all Internet communications. All of them.”47

If this argument is correct, it has significant implications for civil liberties because “[r]elentless assaults on America’s computer networks by . . . foreign governments, hackers and criminals”48 represent a significant threat not only to economic and defense interests but also to personal privacy. A world in which America’s computer networks are constantly being exploited is a world in which Americans’ sensitive data held by banks, hospitals, employers, government agencies, and so forth are at constant risk of being stolen, scrambled, or revealed. Cybersecurity and privacy are often cast as antagonists,49 for plausible reasons. The privacy concerns raised by governmental monitoring of all Internet communications are especially acute. And yet the effective provision of cybersecurity reduces certain sorts of privacy risks even as it generates others. A sense of security about one’s online data is a necessary though insufficient condition for the attainment of privacy in the digital age.50

46 Jack Goldsmith, We Need an Invasive NSA (New Republic, Oct 23, 2013), http://www.newrepublic.com/article/115002/invasive-nsa-will-protect-us-cyber-attacks. As Goldsmith recounts, the previous Director of the NSA reportedly insisted, “I can’t defend the country until I’m into all the networks.” Id (quoting General Keith Alexander).
48 Goldsmith, We Need an Invasive NSA (cited in note 46) (quoting Editorial, Cybersecurity at Risk, NY Times A22 (July 31, 2012)).
49 See, for example, Julia Boorstin, Privacy vs. Cybersecurity: The Debate Heats Up (CNBC, Apr 10, 2013), http://www.cnbc.com/id/100632315.
Is a leading role for the NSA a necessary condition for the effective provision of cybersecurity, however? It is exceedingly difficult to answer this question—and therefore to assess this privacy-privacy tradeoff—because many of the relevant variables are exceedingly complex, counterfactual, or secret. Much more would need to be known about the nature and scope of the cybersecurity threat as it relates to privacy, about the NSA’s distinctive capabilities to combat this threat, and about the privacy protections that would be built into those capabilities. The distributional, dynamic, and dimensional implications of this tradeoff all remain hazy at this time.

The NSA has unique empirical insight into these matters and a political incentive to promote (indeed to overstate) this line of argument—one that recasts the agency as the great protector rather than the great usurper of Americans’ privacy. Perhaps the most that can be said with confidence, then, is that the burden should rest with the NSA to establish the plausibility and desirability of this privacy-privacy tradeoff, and the agency has not yet met that burden.

C. Governmental Custody of Metadata vs. Commercial Custody of Metadata

Of all the NSA activities revealed by Edward Snowden, the one that has elicited fiercest domestic backlash is the agency’s ongoing collection of Americans’ telephone call records under Section 215 of the USA PATRIOT Act. Both the Privacy and Civil Liberties Oversight Board (PCLOB) and the President’s Review Group on Intelligence and Communications Technologies (Review Group) identified the bulk telephony metadata program as a significant threat to privacy with limited security benefit.51 To mitigate this threat, the Review Group urged, the government should transition to a system in which the metadata resides with the communications providers—AT&T, Verizon, and their ilk—or with a newly created independent entity; the NSA would still be able to “query” the information pursuant to an order from the Foreign Intelligence Surveillance Court (FISC), but it would no longer be the custodian.52 “This change,” the Review Group claimed, “would greatly reduce the intake of telephony meta-data by NSA” and “therefore also dramatically . . .

---


reduce the risk, both actual and perceived, of government abuse.”\textsuperscript{53} The leading surveillance reform bill in Congress incorporates this recommendation, with the metadata to be held by the phone companies.\textsuperscript{54}

According to the separate statements filed by two PCLOB members, however, an overlooked privacy-privacy tradeoff threatens to diminish if not reverse the privacy gains this reform is supposed to supply. Mandating that the communications providers retain all telephony metadata, Rachel Brand wrote, “could increase privacy concerns by making the data available for a wide range of purposes other than national security.”\textsuperscript{55} Such data retention requirements, Elisebeth Collins Cook likewise suggested, “would pose separate and perhaps greater privacy concerns.”\textsuperscript{56} In a blog post, Benjamin Wittes fleshed out the case for why this may be “a bad trade purely in civil liberties terms”:

Instead of having one actor with a metadata database—an actor that is politically accountable and subject to all kinds of oversight mechanisms—we would now have . . . several different ones, some with commercial interests. We’d have to build new oversight mechanisms from scratch. . . . It should be a truism that proliferating the number of people and organizations with access to a sensitive database creates proliferating opportunities for abuse by those organizations and people.\textsuperscript{57}

Shifting the metadata database (really, databases) to the private sector might simply shift the locus, and expand the scope, of the privacy threat, at least if the implementing legislation is not well designed. And it might do this while lulling ordinary citizens into believing the threat has been resolved. “If people are concerned about bulk metadata collection and access,” Wittes asks, “does it really make sense to make it more widely available to more people and organizations?”\textsuperscript{58}

The answer depends on normative as well as empirical considerations. Wittes emphasizes the redistributive character of the reform, the way it merely moves the metadata around. But this distributional tradeoff is best understood, I believe, as part of a larger domain tradeoff: Although it may create new possibilities for privacy

\textsuperscript{53}Id at 118.
\textsuperscript{54} USA Freedom Act, HR 3361, 113th Cong, 2d Sess §§ 101–110 (2014).
\textsuperscript{55} PCLOB, Report on the Telephone Records Program at 213 (cited in note 51).
\textsuperscript{56} Id at 214.
\textsuperscript{57} Benjamin Wittes, Assessing the Review Group Recommendations: Part II (Lawfare, Dec 26, 2013), http://www.lawfareblog.com/2013/12/assessing-the-review-group-recommendations-part-ii. As Wittes notes, the recommendation that telephony metadata be held outside the NSA “has played in the press as the heart and soul of the Review Group report.” Id.
\textsuperscript{58} Id. See also 161 Cong Rec S2708 (daily ed May 7, 2015) (Sen. McConnell) (arguing that “[i]n addition to making us less safe, the USA FREEDOM Act would make our privacy less secure” by storing metadata with private companies lacking the NSA’s “rigorous controls”); Examining Recommendations to Reform FISA Authorities, Hearing Before the House Judiciary Committee, 113th Cong, 2d Sess 140–41 (2014) (statement of Steven G. Bradbury) (similar).
infringements by commercial actors, dispersing the metadata would make it more difficult for the NSA to engage in comprehensive data-mining of Americans’ phone records, or to apply that capacity toward a coercive end. A classic liberal fear of centralized authoritarian power is traded off, to some extent, for a more novel and pedestrian fear of decentralized corporate abuse.

Even if Wittes neglects this aspect of the “trade,” however, he is absolutely right that the Review Group’s recommendation implicates a privacy-privacy tradeoff—and that, in consequence, it cannot be taken for granted that the reform would be a boon for privacy. The Review Group’s failure to engage this issue is particularly striking given that its report endorses a holistic approach to risk management, based on the insight that “multiple risks are involved” in NSA surveillance policy, from security to trade to privacy, “and all of them must be considered.”

Faithfully applying this approach requires considering the interactions among not only different categories of risk but also different risks within the category of privacy.

D. Machines vs. Humans (and Bulk Collection vs. Reading and Listening)?

Perhaps the most dramatic privacy-privacy tradeoff concerning NSA surveillance has been suggested by Judge Richard Posner. An opinion piece from 2005 outlines the argument:

The collection, mainly through electronic means, of vast amounts of personal data is said to invade privacy. But machine collection and processing of data cannot, as such, invade privacy. Because of their volume, the data are first sifted by computers, which search for names, addresses, phone numbers, etc., that may have intelligence value. This initial sifting, far from invading privacy (a computer is not a sentient being), keeps most private data from being read by any intelligence officer.

Posner makes two distinct claims about privacy in this passage. First, he contends that machines cannot invade privacy in themselves; only other humans can. (A related position maintains that the collection and processing of metadata cannot, in itself, invade privacy because metadata does not include “content.”) This claim is disputable, but it would be of little moment if the NSA’s machine collection and processing of private communications led to more of those communications being reviewed by an intelligence officer—an activity that, Posner implicitly concedes, plainly does invade privacy. Hence the importance of Posner’s second claim, which


is that the NSA’s vacuuming up of personal data through electronic means can safeguard privacy by reducing the amount of human review.

Restated in more general and prescriptive terms, the suggested tradeoff is that tighter limits on what sorts of data the NSA can electronically collect or mine at the front end might lead to looser—and more privacy-invasive—investigatory practices at the back end. Beyond the automated “sifting” function identified by Posner, a variety of mechanisms could potentially produce such a trade. In the absence of bulk metadata collection under Section 215 of the PATRIOT Act, for instance, the NSA might seek to identify suspected foreign terrorists’ American associates in a less surgical manner, through ever-widening wiretaps instead of link analysis and contact chaining.61 Tighter limits on what may be collected under any particular authority, such as Section 215, could push NSA officers to submit broader warrant applications to the FISC62 or to make greater use of other legal authorities, as by expanding the targeting of non-U.S. persons under Section 702 of the Foreign Intelligence Surveillance Act on the hope or expectation that this would yield more “incidental” collection of U.S. persons’ communications.63 Barriers to domestic acquisition could likewise lead to more aggressive “privacy shopping,” whereby the NSA relies on foreign partners to obtain data it cannot lawfully or efficiently obtain on its own.64

In short, it is not implausible to think that collection limits could backfire; or that the more (meta)data the NSA has at its disposal, the less it will need officers to review intercepted communications. Big Data analytics can take over, to some extent, from old-fashioned listening and reading. And if one deems the latter to be an

61 Government lawyers have gestured at this tradeoff in their public statements about the Section 215 program. See, for example, Robert S. Litt, Privacy, Technology, and National Security, Speech to Brookings Institution *13 (July 19, 2013), online at http://www.lawfareblog.com/wp-content/uploads/2013/07/Bob-Litt-Brookings-Speech1.pdf (“The collection [of metadata] has to be broad to be operationally effective, but it is limited to non-content data . . . . Only the narrowest, most important use of this data is permitted; other uses are prohibited. In this way, we protect both privacy and national security.”). According to Stewart Baker, under its “collection-first model” the NSA has been wiretapping American citizens at a fraction of the rate that its European counterparts have been wiretapping their own citizens. FISA Hearing, 113th Cong, 1st Sess at 77–78 (cited in note 45).

62 See Julian Sanchez, Leashing the Surveillance State 24 (Cato 2011), http://object.cato.org/sites/cato.org/files/pubs/pdf/PA675.pdf (“While it may be tempting to insist that a court order be obtained for all records, this could have the perverse consequence of yielding greater intrusion, as agents would have an incentive to sweep as broadly as possible in a single order . . . even when more-limited records would suffice.”).


especially or uniquely significant privacy problem, one can arrive at the unsettling paradox of preferring that the NSA “collect it all” on privacy grounds.

I want to stress that there are many reasons why this paradox may not obtain in practice and why civil libertarians may decline to trade bulk collection for the hope of downstream privacy benefits. Unless paired with exacting rules regarding how and when data may be accessed, used, shared, and stored—and even if paired with such rules—“collecting it all” could easily lead to more rather than fewer privacy invasions of the sort Posner would recognize. Posner’s conception of what counts as a privacy invasion could also, of course, be rejected in principle. And stringent legal limits on what sorts of data the NSA can acquire and analyze might be designed in ways that are both workable and difficult to circumvent. In any event, the burden must rest heavily upon the NSA to show that its voracious collection practices are a net plus for privacy, relative to a world in which the agency faced greater ex ante constraints. A decade after Posner’s provocation, this burden, too, remains to be met.

IV. IMPLICATIONS AND EXTENSIONS

Although it only scratches the surface of debates over surveillance reform, the discussion in Part III demonstrates that privacy-privacy tradeoffs are deeply (if sometimes inconspicuously) woven into the fabric of these debates. We would find the same thing, Parts I and II indicate, in virtually any area of information policy. How might we build on these observations? If privacy-privacy tradeoffs cannot be avoided, how might they be managed? Some basic suggestions emerge from the analysis above.

First, scholars, advocates, and politicians could do a much better job of identifying and confronting privacy-privacy tradeoffs as tradeoffs. “Unless decisionmakers consider the full set of outcomes associated with each effort to reduce risk,” policy theorists have warned, “they will systematically invite [risk-risk] tradeoffs.” This warning applies equally in the privacy context. Managing privacy-privacy tradeoffs requires attention to (and information about) the full range of privacy interests that may be affected by a decision, the potential conflicts and congruities among those interests, and the expected distribution and degree of privacy gains and losses. It cannot just be assumed that because a certain measure causes privacy harm, even serious harm, privacy would be enhanced overall by

---


66 Graham and Wiener, Confronting Risk Tradeoffs at 2 (cited in note 30). Graham and Wiener propose numerous factors to inform risk tradeoff analysis but caution “that there is no magic recipe. Weighing risks versus risk will often require both objective information and personal judgment, both expert analysis and ethical values.” Id at 19.
jettisoning the measure. Privacy policies and problems cannot be assessed in isolation.

Second, the pluralistic turn in privacy theory may need to be qualified or supplemented in certain respects to accommodate the reality of privacy-privacy tradeoffs. Pluralistic theories of privacy, recall, maintain that there are many different valid understandings of privacy and that none has priority over the others. The ability to control one’s intimate relationships is no more or less central to the right of privacy than the ability to keep secrets or to keep photographers at bay. The danger of this approach is that it increases the likelihood of intra-privacy conflicts (by recognizing more claims as privacy claims) while simultaneously depriving us of the resources to resolve them (by refusing to supply a normative hierarchy of privacy principles). Privacy theory could make itself more relevant to privacy policy by offering guidance on how to weight—or, in cases of incommensurability, how to order—various privacy interests when hard choices must be made among them.

Third, empirical research could assist in this task. Apart perhaps from situations where decisionmakers have a strong deontological commitment to one privacy value over another, they may find it useful to learn how affected parties would assess a tradeoff. And at least in some cases, this information may be attainable. Researchers can ask people whether and to what extent they believe an anticipated privacy-privacy tradeoff would be desirable, and then feed the results into a marginal cost analysis. A pair of computer scientists recently tried this and found, through a simple survey, that many social network users seem eager to trade certain forms of personal information for greater control over photographs in which they appear. The very asking of such questions, moreover, may have the salutary effect of raising anticipated tradeoffs’ salience and fostering debate.

Fourth, Congress, the courts, and the executive branch can take steps to drive attention to privacy-privacy tradeoffs. To a large extent, the question of how to do this is an instance of the larger question of how to structure regulation of risk-risk tradeoffs. Scholars have proposed solutions ranging from greater coordination of risk reduction through the White House’s Office of Information and Regulatory Affairs, to an interpretive principle that agencies are allowed to consider such tradeoffs in the absence of a clear congressional statement to the contrary, to the creation of new congressional committees to handle all risk policy. My own view is that the complexity and ubiquity of privacy-privacy tradeoffs counsel against trusting any

---

67 See text accompanying notes 18–25.
68 In circumstances where a uniform policy is not preferred on ethical, legal, or operational grounds, regulators may be able to go further and give people the option to make their own privacy-privacy tradeoffs, as with the PreCheck program.
69 See note 10.
70 Sunstein, 63 U Chi L Rev at 1537, 1569 (cited in note 13).
71 Id at 1537, 1562–63.
single executive branch institution to make significant decisions affecting privacy. Because each has its own interests, culture, and constituency, any given institution is liable to discount or overlook at least one side of any given tradeoff.

Whatever the best institutional design for regulating risk in general, at least two factors distinguish the case of privacy-privacy tradeoffs. One is that the executive branch already contains numerous entities, such as PCLOB and the Department of Homeland Security’s Privacy Office, with the specific mission of protecting privacy and civil liberties.73 These entities are obvious candidates to promote the study of privacy-privacy tradeoffs and counter possible biases of national security decisionmakers. Reforms that encourage or require these entities to address privacy-privacy tradeoffs, and that enhance their influence on their policy process, could help in this cause.

Another partially differentiating factor is the relationship of privacy and secrecy. Some of the most pressing threats to privacy are now thought to come from the most secretive executive agencies and activities, as exemplified by NSA surveillance. Controlling these agencies, and thus controlling the threat to privacy, requires among other things meaningful congressional oversight and transparency. And yet the lurking tradeoff here is that, unless designed with care, oversight and transparency can themselves put privacy at risk. Both involve, sometimes quite literally, more actors who can see what the regulated party is doing, which in turn may involve more actors looking at sensitive personal information in the latter’s possession.74 There is no global solution to this problem, but it can be managed through policies that provide for partial disclosure, de-identification of personal data, and the like.

Finally, it is important to remain on guard against false tradeoffs and exaggerated countervailing risks in debates over privacy reform. As Albert Hirschman has observed, the allegation that a progressive proposal will have perverse effects is a classic reactionary refrain.75 The mere fact that privacy-privacy tradeoffs are widespread does not imply that existing practices have struck an appropriate balance or that privacy-superior alternatives are unattainable.76 By attending to these tradeoffs, we may well find that existing practices are more problematic for privacy than they had seemed. The privacy-privacy tradeoffs considered in this Essay are not logical truths, inherent in the very concept of privacy. They are practical and socially situated relationships—the product of legal, institutional, and cultural variables, at

73 For an illuminating study of such entities, see Margo Schlanger, Office of Goodness: Influence Without Authority in Federal Agencies, 36 Cardozo L Rev 53 (2014).
74 Cf note 28 (noting a parallel tension between privacy and open-records laws).
76 Cf. Graham and Wiener, Confronting Risk Tradeoffs at 37–39 (cited in note 30) (discussing conditions under which “risk-superior moves are achievable”). Nor does it imply, for that matter, that all unintended consequences will be undesirable. Interventions designed to protect one sort of privacy may turn out to reinforce rather than undercut other sorts of privacy.
least some of which can be tweaked. When it seems like a privacy-superior tradeoff can be made at acceptable cost to other values, it should be.

CONCLUSION

Privacy theorists have lamented that, from safety to efficiency to entrepreneurship, the “list of privacy’s [perceived] counterweights is long and growing.” Even if some items on this list deserve to be removed or demoted, however, one more must be added: privacy itself. This Essay has explored some of the many ways in which interventions that strengthen privacy on one margin can end up weakening it on another.

There is nothing lamentable about this insight; on the contrary, it offers a way forward for theory and advocacy. Privacy-privacy tradeoffs require recognition, study, and debate. Their existence does not make the pursuit of privacy any less urgent, or any more quixotic. Tradeoffs asserted to justify the status quo must be scrutinized with particular care. But if we wish to minimize threats to civil liberties in an age of surveillance, we have no choice but to try to make the best privacy-privacy choices we can.