2016

Privacy-Privacy Tradeoffs

David E. Pozen
Columbia Law School, dpozen@law.columbia.edu

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 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, illuminates 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

† Associate Professor, Columbia Law School. I am grateful to Alvaro Bedoya, Jessica Bulman-Pozen, Josh Chafetz, Matthew Connelly, Jennifer Daskal, Michael Farbiarz, Michael Graetz, Rebecca Ingber, Jeremy Kessler, Daryl Levinson, Henry Monaghan, Deborah Pearlstein, Neil Richards, Daniel Richman, Julian Sanchez, Shirin Sinnar, Ganesh Sitaraman, Lior Strahilevitz, Matthew Waxman, and my co-symposiasts for helpful comments and conversations.

1 See Julie E. Cohen, *Configuring the Networked Self: Law, Code, and the Play of Everyday Practice* 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: Policy Instruments in Global Perspective* 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: Technology, Policy, and the Integrity of Social Life* 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 A. Baker, *Skating on Stilts: Why We Aren't Stopping Tomorrow's Terrorism* 313–15 (Hoover 2010).

imagined) antinomies.[6] Privacy is constantly being juxtaposed with competing goods and interests, balanced against disparate needs and demands. Legal and policy debates about privacy revolve around these tradeoffs.

But privacy also clashes with itself. That is to say, in myriad social and regulatory contexts, enhancing or preserving privacy along a certain axis may entail compromising privacy along another axis. If they wish to be more analytically rigorous, theorists and decisionmakers must take such *privacy-privacy tradeoffs* into 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 unexpected and unwanted. When EU citizens began exercising their right to be forgotten last year and flooded Google with "delete me" requests, the deleted links quickly reappeared—together with the relevant search terms—on a website devoted to documenting Internet censorship.[7] These citizens' bid for online privacy thus seems to have triggered the Streisand effect, "whereby an attempt to suppress a disclosed item of information only draws more attention to it."[8] Other times, privacy-privacy tradeoffs are consciously cultivated and promoted. 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."[9] Enhanced governmental access to your data can be traded for reduced access to your body and belongings.

In many cases, privacy-privacy tradeoffs simply follow from scarce resources and opportunity costs. A tenant on a fixed

---

[5] See generally, 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 generally Lior Jacob Strahilevitz, *Privacy versus Antidiscrimination*, 75 U Chi L Rev 363 (2008).

[7] See Jeff John Roberts, *"Hidden from Google" Shows Sites Censored under EU's Right-to-Be-Forgotten Law* (Gigaom, July 16, 2014), archived at http://perma.cc/8P26-H4YL.

[8] David E. Pozen, *The Leaky Leviathan: Why the Government Condemns and Condones Unlawful Disclosures of Information*, 127 Harv L Rev 512, 558 n 241 (2013), citing *What Is the Streisand Effect?* (The Economist, Apr 15, 2013), archived at http://perma.cc/6TDU-ZBFW.

[9] Mark Johanson, *7 Questions about TSA's PreCheck Program Answered* (International Business Times, Sept 4, 2013), archived at http://perma.cc/NRD7-QS52. This is a privacy-convenience tradeoff as well as a privacy-privacy tradeoff.

budget who spends money soundproofing her walls will have less to spend on mending her curtains. Alternatively, these tradeoffs may be caused by behavioral responses and dynamic feedback effects. Increasing airline passengers' 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 is redistributed across different aspects or bearers of privacy. By establishing a forensic DNA database, law-enforcement officials may impair the privacy of everyone whose DNA is included but protect the privacy of a smaller group of individuals who will not be needlessly investigated for the crimes of others. By "stripping network users of any privacy or anonymity" when they are online,[10] an intelligence agency may deter its analysts 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.[11]

While the idea of privacy-privacy tradeoffs appears to be new to the legal literature,[12] the basic logic behind the idea is not. Criminal law scholars have called attention to the ways in which police practices advantage certain privacy interests at the expense of others.[13] And theorists in law and other disciplines

---

10 Baker, *Skating on Stilts* at 340 (cited in note 4).

11 See Evan Perez, *NSA: Some Used Spying Power to Snoop on Lovers* (CNN, Sept 27, 2013), archived at http://perma.cc/T69M-SZXG.

12 I have found only one prior work that examines privacy-privacy tradeoffs as such: a paper by computer scientists reporting the results of a survey that asked participants about their willingness to share with a social network certain information—photographs, "friend" lists, or their current location—in exchange for notifications about other users' photographs in which the participants might appear. See generally Benjamin Henne and Matthew Smith, *Awareness about Photos on the Web and How Privacy-Privacy-Tradeoffs Could Help*, in Andrew A. Adams, Michael Brenner, and Matthew Smith, eds, *Financial Cryptography and Data Security* 131 (Springer 2013). See also text accompanying notes 87–88 (suggesting extensions of this research). The possibility of privacy-privacy tradeoffs is implicitly recognized in numerous other works. See, for example, Benjamin Wittes and Jodie C. Liu, *The Privacy Paradox: The Privacy Benefits of Privacy Threats* *3 (Brookings Institution, May 2015), archived at http://perma.cc/P28P-VPLC (arguing that "technologies often offer privacy with one hand while creating privacy risks with the other").

13 See generally, for example, Jacqueline E. Ross, Book Review, *Tradeoffs in Undercover Investigations: A Comparative Perspective*, 69 U Chi L Rev 1501 (2002) (surveying competing techniques used in undercover policing, including several—such as electronic surveillance versus infiltration—that implicate privacy-privacy tradeoffs); William J. Stuntz, *The Distribution of Fourth Amendment Privacy*, 67 Geo Wash L Rev 1265 (1999) (criticizing Fourth Amendment law's focus on privacy as shifting legal protection from poorer to wealthier suspects).

have begun to explore "security-security tradeoffs,"[14] "liberty-liberty tradeoffs,"[15] "health-health tradeoffs,"[16] "democracy-democracy tradeoffs,"[17] 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 shows, can clarify and enrich debates over the activities of the NSA as well as over privacy policy generally. Reconceptualizing these debates as pitting privacy against privacy enables more productive consequentialist and critical analysis, and it might even help to disentrench some of the political and ideological divisions that have hardened around privacy-versus-security, privacy-versus-technology, and other conventional frameworks.

This Essay offers no general solution to sort out these tradeoffs, as I am doubtful that there is one to be had. I have become increasingly convinced, however, that we cannot make headway on many privacy problems unless we understand the privacy-privacy tradeoffs at stake. The Essay aspires, above all, to frame and provoke ongoing discussion toward that end.

---

[14] See, for example, Stephen Holmes, *In Case of Emergency: Misunderstanding Tradeoffs in the War on Terror*, 97 Cal L Rev 301, 318–23 (2009).

[15] See, for example, Adrian Vermeule, *A New Deal for Civil Liberties: An Essay in Honor of Cass R. Sunstein*, 43 Tulsa L Rev 921, 922–25 (2008).

[16] See generally, for example, Cass R. Sunstein, *Health-Health Tradeoffs*, 63 U Chi L Rev 1533 (1996).

[17] See, for example, Robert E. Goodin, *Global Democracy: In the Beginning*, 2 Intl Theory 175, 179 n 11 (2010).

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.[18] It is a commonplace in the privacy literature to bemoan the "bewildering variety of meanings" the concept has accumulated.[19] 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."[20]

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 umbrella term that encompasses a variety of related meanings."[21] 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 philosopher Ludwig Wittgenstein's notion of family resemblances, Solove forcefully argues against conceptualizing privacy through a priori generalizations, such as

---

18 Daniel J. Solove, *Understanding Privacy* 1 (Harvard 2008).

19 Neil Richards, *Intellectual Privacy: Rethinking Civil Liberties in the Digital Age* 8 (Oxford 2015). See also, for example, Robert C. Post, *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.").

20 Nissenbaum, *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 nonprivacy terms—has largely lost out in academic as well as popular commentary. See generally *Privacy* (Stanford Encyclopedia of Philosophy, Aug 9, 2013), archived at http://perma.cc/VUZ2-WLXD (explaining that, against the reductionists, "most theorists take the view that privacy is a meaningful and valuable concept").

21 Richards, *Intellectual Privacy* at 9 (cited in note 19). See also *Privacy* at § 3.6 (cited in note 20) (discussing a range of theorists who "defend the view that privacy has broad scope, inclusive of the multiple types of privacy issues described by the [US Supreme] Court, even though there is no simple definition").

necessary and sufficient conditions, in favor of a pluralistic, "bottom up" approach focused on "privacy problems."[22]

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."[23] 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 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.[24] 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."[25]

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

1. Information collection
    - Surveillance
    - Interrogation
2. Information processing
    - Aggregation
    - Identification
    - Insecurity
    - Secondary use
    - Exclusion
3. Information dissemination
    - Breach of confidentiality
    - Disclosure
    - Exposure
    - Increased accessibility

---

[22] Solove, *Understanding Privacy* at 8–9 (cited in note 18). For an expanded discussion of this pluralistic understanding of privacy, see id at 39–77.

[23] Id at 12–37.

[24] Kendall Thomas, *Beyond the Privacy Principle*, 92 Colum L Rev 1431, 1443–48 (1992).

[25] Cohen, *Configuring the Networked Self* at 126, 149 (cited in note 1).

Blackmail
Appropriation
Distortion

4. Invasion
Intrusion
Decisional interference[26]

For the purposes of this Essay, it does not much matter whether these classifications are compelling in all particulars[27] or whether the messiness and complexity of privacy will ever be fully elucidated. 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."[28] This capaciousness exacerbates the dilemma of privacy-privacy tradeoffs. The more sorts of privacy claims that there are, the greater the risk that there will be conflicts among them.[29]

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.[30] As privacy problems, surveillance and interrogation are plausible substitutes. Tightening the rules on criminal interrogation, consequently, could lead to a net

---

26 Solove, *Understanding Privacy* at 10–11 (cited in note 18). See also id at 101–70 (elaborating this taxonomy).

27 For a critique of Solove's approach, see M. Ryan Calo, *The Boundaries of Privacy Harm*, 86 Ind L J 1131, 1139–42 (2011).

28 Solove, *Understanding Privacy* at 101–02 (cited in note 18).

29 See 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.'").

30 On similar logic, former FBI director J. Edgar Hoover reportedly "opposed the internment of Japanese-Americans during World War II, believing the intelligence capabilities of the FBI to be sufficient to locate any risk that might emerge from that community." Samuel J. Rascoff, *Domesticating Intelligence*, 83 S Cal L Rev 575, 609 n 126 (2010).

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.[31] And that threat has no force once a given datum has become public. Voluntary divulgences about one's personal life can be self-protective for this reason. Such divulgences, on some accounts, are a defining feature of our digital age. 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"[32]—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,[33] but these examples suffice to make the point. Solove offers his taxonomy to "enable courts and policymakers to better balance privacy against countervailing interests."[34] The very breadth of the taxonomy underscores the need to start balancing privacy against itself.

II. TRADEOFF TYPES AND TRIGGERS

When exactly does the need to balance privacy against privacy 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 illuminate the structure of the problem.[35]

---

31 Solove, *Understanding Privacy* at 105 (cited in note 18).

32 Bernard E. Harcourt, *The Expository Society: Spectacle, Surveillance, and Exhibition in the Neoliberal Age of* Big Data *11 (Sciences Po Faculty Workshop in Political Theory, Nov 10, 2014), archived at http://perma.cc/5BVF-9V3F.

33 To take just one recurring case suggested by Solove's earlier work, facilitating public access to documents that are held in government databases might reduce the privacy problem of "exclusion," or "the failure to provide individuals with notice and input about their records," while increasing the risk that personal information will be disclosed or exposed to others. Solove, *Understanding Privacy* at 134 (cited in note 18). See also Daniel J. Solove, *The Digital Person: Technology and Privacy in the Information Age* 150–54 (NYU 2004) (discussing potential tensions between privacy and open-access laws).

34 Solove, *Understanding Privacy* at 10 (cited in note 18).

35 For a valuable typology of risk-risk tradeoffs, see John D. Graham and Jonathan Baert Wiener, *Confronting Risk Tradeoffs*, in John D. Graham and Jonathan Baert Wiener,

Governmental entities and corporations maintain countless policies that have implications for privacy.[36] A decision to change, or not to change, any given policy can occasion at least five 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 relies on ethnic profiling to redeploy agents from streets and sidewalks to Islamic cultural centers, Muslim New Yorkers may experience a (significant) loss of privacy while everyone else experiences a (marginal) gain. We can call these sorts of privacy-privacy tradeoffs *distributional tradeoffs*.[37]

Second, risk may be shifted not only among groups that suffer privacy harms but also among groups that *cause* harm to a certain privacy interest—among privacy violators as well as victims. An e-reader such as 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.[38] We can call these sorts of tradeoffs *directional tradeoffs*, to reflect that the privacy threat has been redirected so that it comes from one source instead of another.

Third, 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,

---

eds, *Risk versus Risk: Tradeoffs in Protecting Health and the Environment* 1, 22–25 (Harvard 1995). For a valuable "conceptual map" of health-health tradeoffs, see Sunstein, 63 U Chi L Rev at 1538–42 (cited in note 16).

36 Again, governmental decisions are the focus of this Essay, although privacy-privacy tradeoffs commonly arise from individual and corporate decisions as well.

37 Professor Strahilevitz provides a wide-ranging survey of privacy policy's distributive implications, with numerous examples that may involve privacy-privacy tradeoffs, in Lior Jacob Strahilevitz, *Toward a Positive Theory of Privacy Law*, 126 Harv L Rev 2010 (2013).

38 See Richards, *Intellectual Privacy* at 128–29 (cited in note 19). Benjamin Wittes and Jodie 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, *The Privacy Paradox* at *10 (cited in note 12). See also Orin S. Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, 125 Harv L Rev 476, 512–17 (2011) (presenting the telephone as an example of how emerging technologies may enable new modes of surveillance while allowing for the circumvention of others).

customers, employees, or the like at a threshold stage, on the promise of reduced scrutiny thereafter.[39] Maximalist privacy policies, as suggested in the Introduction's airline example,[40] 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.[41] We can call these sorts of tradeoffs *dynamic tradeoffs*.

Fourth, a policy may shift risk across different privacy interests. Recall the six conceptions of privacy and sixteen categories of "privacy problems" that Professor Solove has identified.[42] 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 service members 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.[43] 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, bystanders, and officers who may be captured on film.[44] Targeting one privacy risk creates a new, countervailing risk. We can call these sorts of tradeoffs *dimensional tradeoffs*.

---

39 See text accompanying note 9 (describing PreCheck). PreCheck also trades off different privacy interests (roughly, personal information for physical intrusion) and may tend to intensify screening of non-PreCheck passengers—making it a dynamic, dimensional, and distributional tradeoff all at once.

40 See text accompanying notes 9–10.

41 Individual 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 the content of her communications from the gaze of the intelligence services but flag her as a suspicious type, deserving of future scrutiny. See Mathew J. Schwartz, *Want NSA Attention? Use Encrypted Communications* (InformationWeek, June 21, 2013), archived at http://perma.cc/XX84-RSWZ (discussing actions that NSA analysts are authorized to take when encryption is encountered).

42 See text accompanying notes 23–26.

43 See Kenji Yoshino, *Assimilationist Bias in Equal Protection: The Visibility Presumption and the Case of "Don't Ask, Don't Tell"*, 108 Yale L J 485, 544–50 (1998) (analyzing the "evasive" advantages and disadvantages of Don't Ask, Don't Tell). See also text accompanying notes 23–25 (noting the existence of decisional, dignitarian, and relational, as well as secrecy-centered, conceptions of privacy).

44 See Rachel Weiner, *Police Body Cameras Spur Privacy Debate* (Wash Post, Nov 10, 2013), archived at http://perma.cc/PT9L-MJUK (discussing these privacy concerns and noting the American Civil Liberties Union's ambivalent support for on-body police cameras).

Certain dimensional tradeoffs recur regularly. State interventions to secure legal privacy rights, for instance, tend to butt up against people's confidentiality and concealment interests. Government surveillance aspires to deter a wide range of privacy crimes through the very act of impinging on privacy.[45] A call to the police after a burglary may well bring more unwelcome visitors into one's home. And government subsidies that enhance recipients' so-called decisional privacy often come with an informational privacy "tax." The Hyde Amendment has restricted the Department of Health and Human Services from funding abortion care for Medicaid recipients since 1976.[46] This refusal to subsidize marks a defeat for decisional privacy in that it impedes women's exercise of their right to obtain an abortion; but it carries at least some benefit for informational privacy in that once the government is no longer paying for abortions, there is necessarily less official data collection about who obtains them and under what circumstances.

Finally, when the traded-off risks are understood to be 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."[47] Perhaps the privacy problems caused by abortion restrictions and government record keeping are immiscible in this way.[48]

---

[45] See Part III.B.

[46] Act of Sept 30, 1976 § 209 ("Hyde Amendment"), Pub L No 94-439, 90 Stat 1418, 1434. I thank Lior Strahilevitz for suggesting this example, among others.

[47] Cass R. Sunstein, *Incommensurability and Valuation in Law*, 92 Mich L Rev 779, 796, 798 (1994) (emphasis omitted) (defining incommensurability in a "very thin" 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. See Sunstein, 63 U Chi L Rev at 1552 (cited in note 16) (observing that "problems of incommensurability . . . play a large role in health-health comparisons" and "certainly" cannot be eliminated).

[48] But see Matthew B. Kugler, *Affinities in Privacy Attitudes: A Psychological Approach to Unifying Informational and Decisional Privacy* *11–39 (unpublished manuscript, July 21, 2014), archived at http://perma.cc/JVZ6-VPFZ (exploring psychological connections between decisional and informational privacy); Neil M. Richards, Book Review, *The Information Privacy Law Project*, 94 Georgetown L J 1087, 1102–21 (2006)

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 of privacy quite directly when implemented, as in the case of police body cameras.[49] 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.[50] Vulnerable actors may overestimate a measure's benefits and be lulled into reducing their own precautions.[51] Strategic actors may exploit the rigidities caused by privacy protections in ways that render them unsustainable.[52] 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;[53] 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 ways to carve up the landscape,[54]

(exploring doctrinal and theoretical connections between decisional and informational privacy).

49 See Samuel J. Rascoff and Richard L. Revesz, *The Biases of Risk Tradeoff Analysis: Towards Parity in Environmental and Health-and-Safety Regulation*, 69 U Chi L Rev 1763, 1771–75 (2002) (classifying such tradeoffs as "direct risk tradeoffs" and noting that paradigmatic examples include "the negative side effects associated with medical interventions").

50 See text accompanying notes 29–30 (giving the hypothetical example of a police force ramping up surveillance in response to new restrictions on interrogation).

51 See Rascoff and Revesz, 69 U Chi L Rev at 1777–78 (cited in note 49), quoting W. Kip Viscusi, *Fatal Tradeoffs: Public and Private Responsibilities for Risk* 225 (Oxford 1992) (discussing "lulling effects," whereby the "introduction of a safety measure . . . can have the effect of 'produc[ing] misperceptions that lead consumers to reduce their safety precautions because they overestimate the product's safety'").

52 See text accompanying notes 9–10 (noting possible iterated interactions between airline passengers' privacy levels and terrorist threats).

53 See Stephen Holmes and Cass R. Sunstein, *The Cost of Rights: Why Liberty Depends on Taxes* 125–26 (Norton 1999) (explaining that "the problem of selective attention" can both generate and obscure rights-rights and risk-risk tradeoffs); 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).

54 Among other possibilities, each of the tradeoff types outlined above might be further sliced on the basis of the number of persons affected, the role of governmental versus nongovernmental actors, or the expected probability and salience of privacy gains and losses. Be that as it may, I believe these categories capture key structural features of privacy-privacy tradeoffs and so supply a useful if limited tool kit for analyzing this heterogeneous phenomenon.

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

Tradeoff Type	Traded-Off Element	Trigger
Distributional	Privacy Victims	Changed Circumstances Direct Effects Error Feedback Effects Ignorance Lulling Effects Opportunity Costs Substitution Effects
Directional	Privacy Violators	
Dynamic	Time Periods	
Dimensional	Privacy Interests	
Domain	Qualitatively Distinct Privacy Interests	

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 an alleged national-security need but also to a privacy-privacy tradeoff.[55] 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 cannot be fairly assessed—or compellingly countered—without an understanding of the privacy-privacy tradeoffs on which they are premised.

A. NSA Analysts versus Ordinary Citizens?

We have already touched on one such argument in defense of NSA surveillance: the contention that by minimizing the network privacy of its own employees and contractors, the NSA can safeguard the communications privacy of everyone else.[56] Former

[55] An additional example of an alleged privacy-privacy tradeoff involving the NSA is discussed in note 94.

[56] See text accompanying notes 10–11.

NSA general counsel Stewart Baker has proposed that this tradeoff be made the centerpiece of any new reforms. "The short answer," Baker suggests, is that "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."[57] Applying this approach, the NSA would "track every database search made by every user," and then "follow any distribution of that data outside the system."[58]

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 also 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 enhance ordinary citizens' privacy only with respect to the rogue behaviors of individual NSA analysts. As a distributional tradeoff, the proposal seems stark; but as a dimensional tradeoff, the proposal is quite limited. Although this may be a trade worth making, it is not responsive to many of the privacy concerns animating the reform movement.

---

57 Baker, *Skating on Stilts* at 321 (cited in note 4).

58 Id. See also id at 340–41 (expanding on this idea); *The Administration's Use of FISA Authorities: Hearing before the Committee on the Judiciary, House of Representatives*, 113th Cong, 1st Sess 75 (2013) ("FISA Hearing") (statement of Stewart A. Baker) (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"); Jack Goldsmith, *The Cyberthreat, Government Network Operations, and the Fourth Amendment* *16 (Brookings Institution, Dec 8, 2010), archived at http://perma.cc/Q3KWCNSX, citing David Brin, *The Transparent Society: Will Technology Force Us to Choose between Privacy and Freedom?* (Addison-Wesley 1998) (noting, in a discussion of cybersecurity surveillance, that the government could "employ David Brin's strategy of snooping on itself to ensure that it does not go further than necessary in snooping on its citizens").

B. Cybersecurity versus Cybersurveillance?

The argument just reviewed envisions the NSA as the guardian of Americans' privacy vis-à-vis internal threats posed by its own badly behaving employees. Another—more challenging and ambitious—argument made by the NSA's defenders envisions the agency as the guardian of Americans' privacy vis-à-vis external threats to cybersecurity. "To keep our computer and telecommunication 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] find reprehensible when done for counterterrorism ends."[59] Specifically, the FBI's general counsel has suggested that "the government needs to be able to monitor all Internet communications. All of them."[60]

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"[61] 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,[62] 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 if insufficient condition for the attainment of privacy in the digital age.[63]

---

[59] Jack Goldsmith, *We Need an Invasive NSA* (New Republic, Oct 10, 2013), archived at http://perma.cc/PP9F-CRUV. As Goldsmith recounts, the previous director of the NSA is said to have insisted: "I can't defend the country until I'm into all the networks." Id (quoting General Keith Alexander).

[60] James A. Baker, *National Security and the Constitution* *8 (Clarke Forum for Contemporary Issues, Sept 12, 2013), archived at http://perma.cc/6CU5-JBPW. Baker sympathetically highlighted this position without committing to it. See id.

[61] Goldsmith, *We Need an Invasive NSA* (cited in note 59), quoting Editorial, *Cybersecurity at Risk* (NY Times, July 31, 2012), archived at http://perma.cc/NS6Z-VQTW.

[62] See, for example, Julia Boorstin, *Privacy vs. Cybersecurity: The Debate Heats Up* (CNBC, Apr 10, 2013), archived at http://perma.cc/VPF6-27PU (highlighting the privacy concerns raised by a 2013 cybersecurity bill).

[63] See Solove, *Understanding Privacy* at 126–29 (cited in note 18) (discussing privacy harms caused by "insecurity," or lack of protection against data leakage, contamination,

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 the 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 met that burden.

C. Governmental Custody of Metadata versus Commercial Custody of Metadata?

Of all the NSA activities revealed by Edward Snowden, the one that elicited fiercest domestic backlash was the agency's ongoing collection of Americans' telephone call records under § 215 of the USA PATRIOT Act of 2001.[64] 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

---

and theft). The security-versus-surveillance tradeoff is by no means confined to the NSA or to the digital realm, and it has many private sector manifestations as well. At this writing, for instance, AT&T and other companies are reportedly developing services that will enable customers to limit their exposure to identity theft by allowing credit card issuers to track, in real time, the geolocation of their phones. See Mikael Ricknäs, *AT&T Wants to Improve Overseas Credit-Card Fraud Prevention via Phone Geolocation* (PCWorld, June 5, 2014), archived at http://perma.cc/M7LK-44SL. Professor William H. Simon has recently suggested that the severe privacy harms caused by the illicit recording and distribution of people's intimate conduct "can only be restrained if the wrongdoers can be identified" through government surveillance. William H. Simon, *Rethinking Privacy* (Boston Review, Oct 20, 2014), archived at http://perma.cc/5YDG-MK47.

64 Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 ("USA PATRIOT Act") § 215, Pub L No 107-56, 115 Stat 272, 287–88, codified as amended at 50 USC §§ 1861–62.

a significant threat to privacy with limited security benefits.[65] To mitigate this threat, the Review Group urged, the government should switch to a system in which the metadata reside either 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.[66] "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."[67] The USA FREEDOM Act of 2015[68] has now enacted a version of this recommendation into law, with the metadata to be held by the phone companies.[69]

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 that this reform is supposed to supply. Having the communications providers retain their customers' metadata in an NSA-friendly format, PCLOB member Rachel Brand wrote, "could increase privacy concerns by making the data available for a wide range of purposes other than national security."[70] In a blog post elaborating on these concerns, Benjamin Wittes argued that "[i]nstead of having one actor with a metadata database—an actor that is politically accountable and subject to all kinds of oversight mechanisms"—

---

65 See *Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court* *12 (PCLOB, Jan 23, 2014), archived at http://perma.cc/ST8L-XRQJ ("The Board also has analyzed the Section 215 program's implications for privacy and civil liberties and has concluded that they are serious."); *Liberty and Security in a Changing World: Report and Recommendations of the President's Review Group on Intelligence and Communications Technologies* *113 (Dec 12, 2013), archived at http://perma.cc/H9V2-KS4N (stating that the "enormity of the breach of privacy caused by queries of [a] hypothetical mass information database," of the sort that could conceivably be compiled under § 215, "dwarfs the privacy invasion occasioned by more traditional forms of investigation").

66 *Liberty and Security in a Changing World* at *25, 115–19 (cited in note 65).

67 Id at *118.

68 Pub L No 114-23, 129 Stat 268.

69 USA FREEDOM Act §§ 101–07, 129 Stat at 269–74, to be codified at 50 USC § 1861. The USA FREEDOM Act does not, however, impose new data-retention obligations on the phone companies beyond what is already required by federal law.

70 *Report on the Telephone Records Program* at *213 (cited in note 65). Such an approach, PCLOB member Elisebeth Collins Cook likewise suggested, "would pose separate and perhaps greater privacy concerns." Id at *218.

the Review Group's proposal could "proliferat[e] the number of people and organizations with access" to sensitive data.[71]

As these critiques suggest, keeping the metadata with the private sector or with some newly created entity might merely shift the locus (and expand the scope) of the privacy threat, at least if the implementing rules are not well designed. A private sector model might also open the door to a richer array of queries if additional phone companies are included in the program[72] or if the companies collect certain information, such as cell phone location data, that the NSA did not collect in bulk. And it might do this while lulling ordinary citizens into believing the privacy threat has been resolved. Add this all up, and one may wonder whether the Review Group has proposed "a bad trade purely in civil liberties terms."[73]

The answer depends on normative as well as empirical considerations. Critics have characterized the Review Group's proposal as redistributing privacy risk from suspected terrorists' associates to the general population. Yet in the absence of a new third-party database or new data-retention requirements, it is not clear that this reform will in fact generate or exacerbate significant privacy vulnerabilities.[74] Moreover, any distributional tradeoff that does occur is best understood, I believe, as part of a larger directional and domain tradeoff: although it creates possibilities for privacy infringements by commercial actors, dispersing the metadata makes it more difficult for the NSA to engage in comprehensive data mining of Americans' phone records

---

71 Benjamin Wittes, *Assessing the Review Group Recommendations: Part II* (Lawfare, Dec 26, 2013), archived at http://perma.cc/DJ3Z-BG2G. As Wittes noted, the recommendation that telephony metadata be held outside the NSA "played in the press as the heart and soul of the Review Group report." Id.

72 See Charlie Savage, *Power Wars: Inside Obama's Post-9/11 Presidency* 608 (Little, Brown 2015) (observing that the Obama administration's § 215 reform plan "would make the NSA more powerful" in one sense, "by permitting the government to include," for the first time, "every phone company in the revamped program").

73 Wittes, *Assessing the Review Group Recommendations* (cited in note 71). See also, for example, NSA Counterterrorism Program, 114th Cong, 1st Sess, in 161 Cong Rec S 2708 (daily ed May 7, 2015) (statement of Senator Mitch McConnell) (contending that "[i]n addition to making us less safe, the USA FREEDOM Act would make our privacy less secure" by leaving the metadata with companies that lack the NSA's "rigorous controls"); Bruce Schneier, *Let the NSA Keep Hold of the Data* (Slate, Feb 14, 2014), archived at http://perma.cc/UCQ3-C6BD (arguing that the Review Group's proposal "makes things worse in several respects" from the perspective of privacy and data security).

74 See Lauren Carroll, *Lindsey Graham: Freedom Act Means Less Privacy for Phone Records* (PolitiFact.com, June 4, 2015), archived at http://perma.cc/3RXF-BKJC (disputing Senator Lindsey Graham's claim that the USA FREEDOM Act "undercut[s] privacy" because the law "does not affect how the companies themselves maintain their records").

or to apply that capacity toward a coercive end. A classic liberal fear of centralized authoritarian power has been given precedence over a relatively novel fear of decentralized corporate abuse.

Even if critics like Wittes have neglected this important aspect of the "trade," however, they are right that the Review Group's recommendations could give rise to a privacy-privacy tradeoff—and that, in consequence, it cannot be taken for granted that their adoption would be a boon for privacy. The Review Group's failure to engage with 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 commerce to privacy, "and all of them must be considered."[75] 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 versus Humans (and Bulk Collection versus Reading and Listening)?

Perhaps the most dramatic privacy-privacy tradeoff concerning NSA surveillance has been suggested by Judge Richard Posner. It turns on the consequences of having machines, rather than humans, at the front lines of the agency's operations. 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.[76]

---

[75] *Liberty and Security in a Changing World* at *15, 46–49 (cited in note 65).

[76] Richard A. Posner, *Our Domestic Intelligence Crisis* (Wash Post, Dec 21, 2005), archived at http://perma.cc/YKX3-WV7T. See also Richard A. Posner, *Privacy, Surveillance, and Law*, 75 U Chi L Rev 245, 254–56 (2008) (asserting that "[c]omputer searches do not invade privacy because search programs are not sentient beings" and speculating that "civil libertarians' preoccupation with warrants" might prove harmful "to civil liberties if it induces legislation to expand the reach of the criminal law"). For a similar argument on how computer searches may substitute for more invasive techniques, see Julian Sanchez, *The*

Posner makes two distinct claims about privacy in this passage. First, he contends that machines cannot by themselves invade privacy; only other humans can. (A related position maintains that the collection and processing of metadata cannot, in themselves, invade privacy because metadata do not include "content."[77]) 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 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 conceivably produce such a result. In the absence of bulk metadata collection under § 215 of the USA 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.[78] Tighter limits on what may be acquired under any particular authority, such as § 215, could push NSA officers to submit broader warrant applications to the

---

Pinpoint Search: How Super-Accurate Surveillance Technology Threatens Our Privacy (Reason.com, Jan 10, 2007), archived at http://perma.cc/7WFR-TWQU (quoting Professor Jeffrey Rosen for the view that high-tech "pinpoint" searches should be embraced by the privacy community inasmuch as they can "find illegal activity" without recourse to invasive physical searches).

77 See, for example, Geoff Nunberg, *Calling It 'Metadata' Doesn't Make Surveillance Less Intrusive* (NPR, June 21, 2013), archived at http://perma.cc/PD6X-3DED (quoting Senator Dianne Feinstein as defending the NSA's bulk telephony metadata program on the ground that "[t]here is no content involved").

78 Government lawyers have gestured at this tradeoff in their public statements about the § 215 program. See, for example, Robert S. Litt, *Privacy, Technology and National Security: An Overview of Intelligence Collection* *10 (Office of the Director of National Intelligence, July 19, 2013), archived at http://perma.cc/94AS-BTGU ("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 58) (statement of Stewart A. Baker).

FISC[79] or to make greater use of other legal authorities, as by expanding the targeting of non-US persons under § 702 of the Foreign Intelligence Surveillance Act of 1978[80] (FISA) on the hope or expectation that this would yield more "incidental" collection of US persons' communications.[81] 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.[82]

In short, it is not implausible to worry that collection limits could backfire or to think 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 especially or uniquely significant privacy problem, then one can arrive at the unsettling paradox of preferring that the NSA "collect it all"[83] *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 be wise to 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

---

79 See Julian Sanchez, *Leashing the Surveillance State: How to Reform Patriot Act Surveillance Authorities* *24 (Cato Institute, May 16, 2011), archived at http://perma.cc/Z7B5-FNGV ("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.").

80 Pub L No 95-511, 92 Stat 1783, codified as amended in various sections of Titles 18 and 50. Section 702 of FISA was added by the FISA Amendments Act of 2008 § 101, Pub L No 110-261, 122 Stat 2436, 2437–48, codified as amended at 50 USC § 1881a.

81 See *Report on the Surveillance Program Operated pursuant to Section 702 of the Foreign Intelligence Surveillance Act* *82 (PCLOB, July 2, 2014), archived at http://perma.cc/J42S-RRBZ (discussing the "incidental" collection of US persons' communications and noting that, under the NSA's PRISM program, such collection "is not accidental, nor is it inadvertent").

82 See Didier Bigo, et al, *Mass Surveillance of Personal Data by EU Member States and Its Compatibility with EU Law* *17, 32 (CEPS, Nov 2013), archived at http://perma.cc/6CDD-GKYL (describing "privacy shopping" as a technique by which intelligence agencies such as the NSA "exchang[e] targets of surveillance in order to use the loopholes created in many national privacy laws").

83 Ellen Nakashima and Joby Warrick, *For NSA Chief, Terrorist Threat Drives Passion to 'Collect It All'* (Wash Post, July 14, 2013), archived at http://perma.cc/Z5WP-DFMJ.

principle. And stringent legal limits on what sorts of data the NSA can acquire and analyze might be designed in ways that are both operationally workable and difficult to circumvent. In any event, the burden must rest heavily on the NSA to show that its voracious collection practices have been 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? When privacy-privacy tradeoffs cannot be avoided, how might they be managed? Some basic suggestions emerge from the analysis above.

First, scholars, advocates, and government officials 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."[84] 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 simply be assumed that because a certain measure causes privacy harm, even serious harm, privacy would be enhanced overall by 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

---

[84] Graham and Wiener, *Confronting Risk Tradeoffs* at 2 (cited in note 35). Professors John Graham and Jonathan Wiener propose numerous factors to inform risk-tradeoff analysis but caution "that there is no magic recipe. Weighing risk versus risk will often require both objective information and personal judgment, both expert analysis and ethical values." Id at 19.

privacy, recall, maintain that there are many different valid understandings of privacy and that none has priority over the others.[85] The ability to control one's intimate relationships is no more or less central to the right of privacy than is the ability to keep secrets or to keep photographers at bay. The danger of this approach is that *it increases the likelihood of intraprivacy conflicts* (by recognizing more claims as privacy claims) *while simultaneously depriving us of resources to resolve them* (by refusing to supply a hierarchy of privacy principles). Domain tradeoffs raise especially acute, and on some accounts insuperable, challenges for consequentialist analysis.

Privacy theory could make itself more relevant to privacy policy by offering guidance on how to weigh—or, in cases of incommensurability, how to order—various privacy interests when hard choices must be made among them. These choices are going to be made, wittingly or unwittingly. The overarching question for policymakers is whether privacy-privacy tradeoffs can be handled in a manner that better serves the goals of privacy, however that ideal is understood and integrated with broader goals such as social welfare or distributive justice.[86] The development of normative frameworks for evaluating privacy-privacy tradeoffs is an increasingly urgent task for the privacy field.

Third, empirical research could assist in this task. At least when they do not have an a priori commitment to one privacy value over another, decisionmakers may find it useful to learn how affected parties would assess a tradeoff. And at least in some cases, such learning is possible. Privacy may be notoriously difficult to measure and price in the abstract. But if nothing else, researchers and regulators can ask people whether and to what extent they believe an anticipated privacy-privacy tradeoff would be desirable, or they can design mechanisms that induce people to reveal their privacy preferences, and then feed the results

---

[85] See text accompanying notes 21–29.

[86] There are numerous ways this ideal might be pursued, from conventional cost-benefit analysis, to cost-benefit analysis subject to deontological constraints, to a maximin strategy that seeks to avoid worst possible privacy outcomes or to advance privacy for the most vulnerable groups, to a risk-reduction strategy that seeks to minimize overall risks to privacy, to a more experimentalist approach that continuously assesses privacy practices and reconsiders privacy goals. Resolving privacy-privacy tradeoffs in a systematic fashion requires both a substantive assessment of competing privacy interests and a decision procedure into which those assessments can be fed.

into a marginal cost analysis.[87] 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 the photographs in which they appear.[88] 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 and cost-benefit analysis through the White House's Office of Information and Regulatory Affairs,[89] to an interpretive principle allowing agencies to consider such tradeoffs in the absence of a clear congressional statement to the contrary,[90] to the creation of new congressional committees to handle all risk policy.[91] My own view is that the complexity and ubiquity of privacy-privacy tradeoffs counsel against trusting any 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. It would be a mistake, on this logic, to house cybersecurity and cybersurveillance responsibilities within the same institution.

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 the PCLOB and the Department of Homeland Security Privacy Office, with the specific mission of protecting privacy and civil liberties.[92] These entities are obvious candidates to promote the study of privacy-privacy tradeoffs and to counter possible biases of national-security decisionmakers.

---

87 In circumstances in which 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 resolve their own privacy-privacy tradeoffs, as with the PreCheck program.

88 See note 12.

89 Sunstein, 63 U Chi L Rev at 1537, 1569 (cited in note 16).

90 Id at 1537, 1562–63.

91 Jonathan Baert Wiener and John D. Graham, *Resolving Risk Tradeoffs*, in Graham and Wiener, eds, *Risk versus Risk* 226, 250–51 (cited in note 35).

92 For an illuminating study of such entities, see generally Margo Schlanger, *Offices of Goodness: Influence without Authority in Federal Agencies*, 36 Cardozo L Rev 53 (2014).

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. Through the USA FREEDOM Act, Congress has recently instructed a new class of amici curiae to supply the FISC with "legal arguments that advance the protection of individual privacy."[93] This charge represents a larger delegation of discretion than it might seem, given the many practical and normative tensions that may arise within the category of privacy, and it cannot sensibly be carried out without consideration of privacy-privacy tradeoffs.

Another partially differentiating factor is the relationship between 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 meaningful congressional oversight and transparency. And yet the lurking tradeoff 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.[94] There is no global solution to this problem, but it can be managed through policies that provide for partial disclosure, review of representative samples, de-identification of personal data, and the like.

Finally, it is important to remain on guard against false tradeoffs, exaggerated countervailing risks, and overly reductive logic in debates over privacy reform. Scholars have identified numerous flaws in the conceit of an inherent conflict between

---

[93] USA FREEDOM Act § 401, 129 Stat at 279, to be codified at 50 USC § 1803(i)(4)(A).

[94] See note 33 (noting a parallel tension between privacy and open-records laws). Citing this concern, the NSA has declined to tell Congress how many US persons' communications are "incidentally" collected under FISA § 702 and Executive Order 12333, 3 CFR 200. To derive these figures, the agency maintains, "would actually be invasive of privacy, because it would require government personnel to spend time scrutinizing the contents of private messages that they otherwise might never access or closely review." *Report on the Surveillance Program* at *147 (cited in note 81). The NSA's argument here strikes me as strained, as it seems likely that there are ways these figures could be estimated—and the NSA's operations thus subjected to more exacting scrutiny—without resort to massive human review of collected communications. See Alvaro Bedoya, *Executive Order 12333 and the Golden Number* (Just Security, Oct 9, 2014), archived at http://perma.cc/66BL-BZNM; Timothy B. Lee, *The NSA Could Figure Out How Many Americans It's Spying on. It Just Doesn't Want to.* (Wash Post, Dec 4, 2013), archived at http://perma.cc/ZH5T-V4JP.

privacy and security.[95] An appreciation of privacy-privacy tradeoffs provides yet another reason why the "hydraulic conception"[96] of the privacy-security relationship is misleading: it implicitly assumes that the relevant threats to each value come from the other value, when in reality each may be just as likely to clash with itself. Incremental gains or losses on any given dimension of privacy have no clear-cut implications for the overall state of privacy, much less for the overall state of security.

More broadly, as Professor Albert Hirschman has explained, the allegation that a progressive proposal will have perverse effects is a classic reactionary refrain.[97] 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.[98] 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 concept of privacy. They are practical and socially situated relationships—the product of legal, institutional, and cultural variables, at least some of which can be tweaked. When it seems like a privacy-superior move 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."[99] Even if certain 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.

---

95 For a powerful critique of necessitarian claims about liberty-security tradeoffs, see Holmes, 97 Cal L Rev at 312–18 (cited in note 14).

96 Id at 323.

97 Albert O. Hirschman, *The Rhetoric of Reaction: Perversity, Futility, Jeopardy* 11–42 (Belknap 1991).

98 See Graham and Wiener, *Confronting Risk Tradeoffs* at 37–39 (cited in note 35) (discussing the 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—generating *privacy cascades* rather than privacy-privacy tradeoffs. Exploring the conditions under which privacy cascades are more or less likely to occur might be another fruitful direction for applied privacy theory.

99 Julie E. Cohen, *What Privacy Is For*, 126 Harv L Rev 1904, 1904–05 (2013).

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 vital or any more quixotic. When an agency such as the NSA stands to benefit from an alleged tradeoff, the agency should bear the burden of establishing the validity of the tradeoff as well as the value of the "trade." Privacy-privacy tradeoffs asserted to justify the status quo must be scrutinized with particular care. But the problems posed by these tradeoffs are real and enduring. 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-versus-privacy choices we can.