Beyond Cheneyism and Snowdenism

Very preliminary draft 4/3/2015; subject to revision
All rights reserved
Forthcoming, University of Chicago Law Review
For Symposium to be held at the University of Chicago in June 2015

Beyond Cheneyism and Snowdenism

Cass R. Sunstein*

Abstract

In the domain of national security, many people favor some kind of Precautionary Principle, insisting that it is far better to be safe than sorry, and hence that a range of important safeguards, including widespread surveillance, are amply justified to prevent loss of life. Those who object to the resulting initiatives, and in particular to widespread surveillance, respond with a Precautionary Principle of their own, seeking safeguards against what they see as unacceptable risks to privacy and liberty. The problem is that as in the environmental context, a Precautionary Principle threatens to create an unduly narrow viewscreen, focusing people on a mere subset of the risks at stake. What is needed is a principle of risk management, typically based on some form of cost-benefit balancing. For many problems in the area of national security, however, it is difficult to specify either costs or benefits, creating a severe epistemic difficulty. Considerable progress can nonetheless be made with the assistance of four ideas, calling for (1) breakeven analysis; (2) the avoidance of gratuitous costs (economic or otherwise); (3) a prohibition on the invocation or use of illicit grounds (such as punishment of free speech or prying into people's private lives); and (4) maximin, which counsels in favor of eliminating, or reducing the risk of, the very worst of the worst-case scenarios. In the face of incommensurable goods, however, the idea of maximin faces particular challenges.

I. Two Targets and A Thesis

Consider two views:

[*] Robert Walmsley University Professor, Harvard University. I am grateful to Michelle Gemmell, Heidi Liu, and Mary Schnoor for valuable research assistance, and to Eric Posner and Geoffrey R. Stone for helpful comments. The author served as a member of the President's Review Group on Intelligence and Communications Technologies, which operated from 2013 to 2014. The Final Report of the Review Group can be found at http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf. While fully consistent with the Final Report, this article does not draw on any information obtained as a result of participation in the Review Group and restricts itself to the public record. It should be unnecessary to say that this article has no official status and reflects only the views of the author.

> 1. *The world has become an unprecedentedly dangerous place. Terrorist threats are omnipresent. As the 9/11 attacks display, numerous people are prepared to engage in terrorism, and they sometimes succeed. In particular, they want to kill Americans. The first obligation of public officials is to keep the citizenry safe. To do that, she best methods may well involve widespread surveillance both domestically and abroad. If the result is to save lives, it is worth it. Even when the probability of harm is low, and even if government is operating in the midst of grave uncertainty, it is appropriate to do whatever must be done, and whatever technology allows, to prevent deaths and to protect the nation, even or perhaps especially from worst-case scenarios.*
>
> 2. *Americans face unprecedented threats from their own government. In the aftermath of the 9/11 attacks, the United States has seen the rise of a massive and (at least until recently) mostly secret security apparatus, involving the collection of vast quantities of data involving the communications of ordinary people. Personal privacy is now at serious risk, and the same is true of free speech. "Trust us" is never an adequate response to citizens' legitimate concerns. We need to create aggressive safeguards to protect civil liberties not only now but also for periods in which government is in especially bad hands -- and to create precautions against the evident dangers, including worse-case scenarios.*

For vividness and ease of exposition, and without ascribing particular views to any particular person, we can describe the first position as "Cheneyism," in honor of former Vice President Dick Cheney. Consider his suggestion that "sooner or later, there's going to be another attack and they'll have deadlier weapons than ever before, that we've got to consider the possibility of a nuclear device or biological agent. . . . And when you consider somebody smuggling a nuclear device into the United States, it becomes very important to gather intelligence on your enemies and stop that attack before it ever gets launched."[1] There is a catastrophic worst-case scenario here, in the form of a nuclear device in the hands of terrorists in the United States.

Also for vividness and ease of exposition, and again without ascribing particular views to any particular person, we can describe the second as "Snowdenism," in honor of former National Security Agency contractor Edward Snowden. Consider his suggestion that "if we want to live in open and liberal societies, we need to have safe spaces where we can experiment with new thoughts, new ideas, and [where] we can discover what it is we really think and what we really believe in without being judged. If we can't have the privacy of our bedrooms, if we can't have the privacy of our notes on our computer, if we can't have the privacy of our electronic diaries, we can't have privacy at all."[2] There is a catastrophic worst-case scenario here, in the form of a situation in which "we can't have privacy at all."

[1] http://www.foxnews.com/on-air/fox-news-sunday-chris-wallace/2013/06/16/former-vice-president-dick-cheney-talks-nsa-surveillance-program#p//v/2482865656001

[2] James Bamford and Tim De Chant, *Exclusive: Edward Snowden on Cyber Warfare,* PBS, January 8, 2015, http://www.pbs.org/wgbh/nova/next/military/snowden-transcript/

Both Cheneyism and Snowdenism reflect enthusiasm for aggressive precautions against risks, though they display radically different perspectives on what we have to fear most. My principal goal here is to reject the two approaches and to link them with a standard, but unhelpful, approach to risks in general.[3] I will sketch a behavioral perspective on why that unhelpful approach has such widespread appeal, perhaps especially in the domain of national security. I will suggest that in order to avoid narrow viewscreens, a far better approach focuses on risk management, with a particular focus on cost-benefit analysis. One of the many advantages of a cost-benefit analysis is that it reduces (without eliminating) the twin dangers of selective attention and motivated reasoning.

In the face of high levels of uncertainty, however, that approach faces especially serious challenges, above all because we may not enough to specify either costs or benefits. I will suggest that it is possible to respond to that uncertainty with four ideas: breakeven analysis; the avoidance of gratuitous costs (economic or otherwise); a prohibition on the invocation of certain illicit grounds; and maximin, which requires attention to the worst of the worst-case scenarios. I shall explore how these ideas might help us to get beyond Cheneyism and Snowdenism.

II. An Unhelpful Principle

A. Precautions and Paralysis

In environmental policy, many people accept the Precautionary Principle.[4] The idea takes diverse forms, but the central idea is that regulators should take aggressive action to avoid environmental risks, even if they do not know that those risks will come to fruition and indeed even if the likelihood of harm is very low. Suppose, for example, that there is some probability, even a small one, that genetic modification of food will produce serious environmental harm. For those who embrace the Precautionary Principle, it is important to take precautions against potentially serious hazards, simply because it is better to be safe than sorry. Especially if the worst-case scenario is very bad, strong precautions are entirely appropriate. Compare the medical situation, where it is tempting and often sensible to say that even if there is only a small probability that a patient is facing a serious health risk, doctors should take precautions to ensure that those risks do not come to fruition.

In an illuminating account, the Precautionary Principle is understood as holding "that if an action or policy has a suspected risk of causing severe harm to the public

[3] I discuss and criticize that approach in broad terms in Cass R. Sunstein, Laws of Fear (2006), and draw on that discussion here.

[4] For general discussion, see id.; Kerry Whiteside, Precautionary Politics (2006). An especially interesting discussion is Nassim Nicholas Taleb et al., The Precautionary Principle (with Application to the Genetic Modification of Organisms) (2014), available at http://www.fooledbyrandomness.com/pp2.pdf

domain (affecting general health or the environment globally), the action should not be taken in the absence of scientific near-certainty about its safety. Under these conditions, the burden of proof about absence of harm falls on those proposing an action, not those opposing it."[5] The Wingspread Declaration puts it more cautiously: "When an activity raises threats of harm to human health or the environment, precautionary measures should be taken even if some cause and effect relationships are not fully established scientifically. In this context the proponent of an activity, rather than the public, should bear the burden of proof."[6]

The influential 1992 Rio Declaration states, also with relative caution: "Where there are threats of serious or irreversible damage, lack of full scientific certainty shall not be used as a reason for postponing cost-effective measures to prevent environmental degradation."[7] In Europe, the precautionary principle has sometimes been understood in a still stronger way, suggesting that it is important to build "a margin of safety into all decision making."[8] This stronger version, associated with both Cheneyism and Snowdenism, is what I mean to explore here, in the form of a suggestion that when an activity, product, or situation *might* create risks, it is appropriate to take precautions against those risks, even if the probability of harm is very low.[9]

In the abstract, these ideas have evident appeal. A clear demonstration of imminent or eventual harm is hardly necessary to justify precautions. But there is a serious, even devastating problem with the Precautionary Principle, at least in its crudest forms[10]: Risks are on all sides of social situations, and efforts to reduce risks can themselves create risks. For this reason, the Precautionary Principle forbids the very steps that it requires. If a nation takes aggressive steps against genetic modification of food, it might deprive people, including poor people, of food that is low in cost and high in nutrition. Precautions themselves can create "a risk of significant health or environmental

[5] Taleb et al., supra note. Note that Taleb et al. defend the Precautionary Principle "in extreme situations: when the potential harm is systemic (rather than localized) and the consequences can involve total irreversible ruin, such as the extinction of human beings or all life on the planet."
[6] See http://www.monitor.net/rachel/r586.html
[7] Quoted in Bjorn Lomborg The Skeptical Environmentalist 347 (2001).
[8] See Bjorn Lomborg The Skeptical Environmentalist 348 (2001).
[9] For a valuable and subtle discussion, see Daniel Steel, Risk and the Precautionary Principle (2014). For an instructive challenge to my arguments here, at least in the context of genetically modified organisms, see Taleb et al., supra note. Of course we could imagine varieties of Cheneyism and Snowdenism that take many different forms. They might, for example, suggest that the danger is real and present, and not conjectural or probabilistic. Even in those forms, however, the analysis here is essentially unaffected. As the interest in national security or in privacy protection begins to focus on the full range of variables at stake – including expected outcomes and probabilities – it begins to converge on the risk management approach that I mean to endorse.
[10] There are many refinements. See, e.g., id.; Steel, supra note.

damage to others or to future generations." It follows that the very steps commanded by the Precautionary Principle violate the Precautionary Principle.[11]

The point is general. Whenever a nation adopts new regulation, it will usually impose costs (at least with some probability). Increases in costs can create risks, including potentially catastrophic ones. If, for example, a nation adopts a regulation that costs $1 billion, or even $500 million, there is some danger that it will have significant adverse effects (perhaps through increasing costs to consumers, perhaps through creating job loss, perhaps by causing industries to do business elsewhere) that will have harmful cascade-like consequences. Some straws end up breaking the camel's back, and through processes that are ill-understood, a single-shot intervention can disrupt whole systems, potentially producing catastrophes. The point is that few precautions lack downside risks, and if we are concerned to build a "margin of safety" into all decisions, any such margins must apply to precautions too. Worst-case thinking can be quite dangerous.

For this reason, the Precautionary Principle turns out to be incoherent, even paralyzing, because it forbids the very measures that it requires. Precautions are mandated by the principle, but precautions create risks, and so they simultaneously offend the principle. None of this means, of course, that nations should not be concerned about genetic modification of food, or that they should demand a certainty of harm, or even a probability of harm, before undertaking regulation. If an activity creates a one percent risk (or less) of producing catastrophic environmental damage,[12] then it is worthwhile to expend significant resources to eliminate that risk, even if our only focus is on expected value. People buy insurance against low-probability harms, and sensibly so. But reasonable regulators must consider both sides of the equation. Acknowledging the potential difficulty of valuation, they must engage in some form of risk management, ad consider whether the costs of precautions are worth the benefits, acknowledging that both of those concepts need to be specified.[13]

B. The Appeal of Precautions

These points raise a genuine puzzle: Why do reasonable people accept forms of the Precautionary Principle that do not make much sense? The answers bear directly on environmental policy, but as we shall see, they help to account for the appeal of Cheneyism and Snowdenism as well. The most general point is that the Precautionary Principle seems appealing and workable because and when people use narrow viewscreens, focusing on a subset of the risks at stake, rather than the whole. (There are

[11] Taleb et al., supra note, offers an interesting refinement and counterargument in the case of genetic modification, focused on the risk of truly catastrophic harm. Even if their argument is taken as convincing, it is explicitly limited to unusual contexts, see id., and hence does not bear on the general points made here.

[12] See id.

[13] I am largely bracketing the question of specification here, and also questions about distribution and equity. For a superb discussion, see Matthew Adler, Well-Being and Fair Distribution (2011).

close analogues in the domain of investor behavior.) Narrow viewscreens can also produce *motivated reasoning*. Suppose that we are focused above all on risks associated with terrorism. If so, we might be motivated to discount, and to treat as trivial, the privacy and liberty risks said to be associated with certain measures designed to reduce the risks of terrorism. Or suppose that we are focused above all on privacy and liberty. If so, we might be motivated to discount, and to treat as trivial, the risks said to be associated with certain measures designed to protect against risks to privacy and liberty. In my view, both forms of motivated reasoning play a significant role (and perhaps especially the latter).

Three more particular factors seem especially important. The first is the *availability heuristic*. A risk that is familiar, like the risk associated with nuclear power, will be seen as more serious than a risk that is less familiar, like the risk associated with heat during the summer.[14] So too, recent events will have a greater impact than earlier ones. The point helps explain much risk-related behavior, including decisions to take or to urge precautions. In the aftermath of an earthquake, insurance for earthquakes rises sharply – but it declines steadily from that point, as vivid memories recede.[15] Whether people will buy insurance for natural disasters is greatly affected by recent experiences.[16] If floods have not occurred in the immediate past, people who live on flood plains are far less likely to purchase insurance.[17] In the words of Amos Tversky and Daniel Kahneman, "a class whose instances are easily retrieved will appear more numerous than a class of equal frequency whose instances are less retrievable."[18]

The central point is that for those who embrace the Precautionary Principle, some risks are cognitively available, and others are not. Because the focus is on the former, the principle seems far more coherent than it is. Suppose, for example, that the Precautionary Principle has appeal in the context of nuclear power. The appeal might have a great deal to do with highly salient incidents in which the risks associated with nuclear power came to fruition, or close to it – as in the case of Three Mile Island and Fukushima. Or suppose that the principle seems to suggest the importance of a new initiative to reduce the risk of train accidents. It would not be surprising if those who are motivated by the principle are alert to a recent train accident, appearing to justify precautions.

The second factor involves *loss aversion*.[19] Behavioral scientists have emphasized that people much dislike losses from the status quo. In fact they dislike losses about twice as much as they like corresponding gains. The Precautionary Principle often seems coherent only because losses, or particular losses, are salient, while foregone gains, or other kinds of losses, are not. In the context of genetically modified food, for example,

[14] See Eric Klinenberg, Heat Wave (2000).
[15] Paul Slovic, The Perception of Risk 40 (2000).
[16] Id.
[17] Id.
[18] Amos Tversky and Daniel Kahneman, Judgment Under Uncertainty: Heuristics and Biases 186 Science 1124 (1974).
[19] See Eyal Zamir, Law, Psychology, and Morality: The Role of Loss Aversion (2014).

the environmental risks seem, to many, to be salient and "on-screen," because they are self-evidently losses, while the various costs of regulation might not be, because they prevent potential gains.[20] And in the context of privacy, loss aversion can be especially important, as people strongly resist a loss of privacy that they have come to expect. (The idea of "reasonable expectation of privacy" may, in fact, encode some form of loss aversion.)

The third factor, and perhaps the most important, involves *probability neglect*.[21] The largest point if that if a bad outcome is emotionally gripping, people might well be inclined to eliminate it, even if it has a low probability of coming to fruition. The emotionally gripping outcome crowds out an assessment of the question of probability. And in fact, both Cheneyism and Snowdenism seem to derive a significant amount of their attraction from probability neglect. Suppose that you are asked how much you would pay to eliminate a small risk of a gruesome death from cancer, a terrorist attack, or a fatality risk to a small child. You might well focus on the tragic outcome, and not so much on the question of probability. A great deal of evidence confirms the phenomenon of probability neglect.[22] The Precautionary Principle often has appeal, and seems sensible, because some subset of risks seems emotionally gripping, and the bad outcomes associated with those risks serve to "crowd out" other considerations.

Consider in this regard the finding that when people are asked how much they will pay for flight insurance for losses resulting from "terrorism," they will pay more than if they are asked how much they will pay for flight insurance from all causes.[23] The evident explanation for this peculiar result, fitting with a form of Cheneyism, is that the word "terrorism" evokes vivid images of disaster, thus crowding out probability judgments. Note also that when people discuss a low-probability risk, their concern rises even if the discussion consists mostly of apparently trustworthy assurances that the likelihood of harm really is infinitesmal.[24]

II. Precautions: National Security and Privacy

A. Cheneyism

Some people embrace a version of the Precautionary Principle that no one rejects, which grows out of the self-evident idea that it is exceedingly important to counteract serious threats to the nation, including terrorist attacks. Vice President Cheney himself offered the core of the principle, stating, "We have to deal with this new type of threat in

[20] On the importance of what is on-screen and what is not, see Howard Margolis, Dealing With Risk (1987).
[21] Cass R. Sunstein, Probability Neglect, 112 Yale L.J. 61 (2002).
[22] See id.
[23] See E.J. Johnson et al., Framing, Probability Distortions, and Insurance Decisions, 7 H. Risk and Uncertainty 35 (1993).
[24] See A.S. Alkahami and Paul Slovic, A Psychological Study of the Inverse Relationship Bteween Perceived Risk and Perceived Benefit, 14 Risk Analysis 1086, 1094-94 (1994).

a way we haven't yet defined. . . . With a low-probability, high-impact event like this . . . If there's a one percent chance that Pakistani scientists are helping al Qaeda build or develop a nuclear weapon, we have to treat it as a certainty in terms of our response."[25] In terms of standard decision theory, of course, it seems preposterous to treat a one-percent risk the same way that one would treat a certainty. People should not, and ordinarily do not, live their lives that way. But as the stakes grow higher, the expected value of a one-percent risk becomes higher as well, and a precautionary approach to a one-percent risk of catastrophe has a great deal of appeal.

For purposes of illustration, let us focus on the question of surveillance. Even if some kinds of surveillance sweep up an immense amount of material, including much that has no interest from the standpoint of national security, surely it is better to be safe than sorry. It is tempting to emphasize the great difficulty of ruling out the possibility that if the intelligence community obtains as much information as technology permits, it will find some information that is ultimately helpful for national security purposes. "Helpful" here is not mere abstraction; it may mean "saves lives" or "prevents catastrophes." Perhaps surveillance could prevent another 9/11; perhaps some forms of surveillance have not proved indispensable in the recent past, but perhaps they could prove indispensable in the future. A precautionary measure in ordinary life – say, purchase of safety equipment for a car – is not valueless because it has not proved necessary over the initial years of ownership. It might well be worthwhile if it avoids just one incident at some time during the life of the vehicle.

This claim could be elaborated in different ways, emphasizing diverse consequences from a successful terrorist attack. Whenever such an attack occurs, it has a series of proliferating costs, economic and otherwise. And if a future attack occurs, it might well lead to a demand for further restrictions on civil liberties – meaning that aggressive steps, designed to protect against attacks and in the eyes of some objectionable from the standpoint of civil liberties, might ultimately be justified or even necessary *as a means of protecting civil liberties*. With these points in view, it seems plausible to argue that at least in the context of national security, a Precautionary Principle makes a great deal of sense.

In light of that point, it is similarly tempting to think: If we *can* obtain information, we *should* obtain information. This thought is especially tempting to those whose mission is to protect the nation from harm. If your job is to reduce the risk of terrorist attacks – and if you will be responsible, at least in part, for any such attacks if they occur – you might well want every available tool to increase the likelihood that no attacks will occur on your watch. That attitude might even seem indispensable to successful performance of your most important task.

Here as elsewhere, however, the problem is that multiple risks are involved. The point may be simplest to see when the question involves standard war-making. Any effort to use military force will create obvious risks, including risks to life and limb. What is

[25] See Ron Suskind, The One Percent Doctrine (2007).

required is a balance of risks, including probabilistic ones, rather than abstract invocation of the idea of precaution.

The same point holds true for widespread surveillance, which creates multiple risks of its own.[26] Of these, perhaps the most obvious involve personal privacy. If government holds a great deal of information, there is at least a risk of abuse – perhaps now or soon, but if not, potentially in the future. We could imagine a range of possible fears and threats. Perhaps it is the mere fact of collection that is objectionable. Perhaps public officials are learning, or would learn, about interactions or relationships for which people have a reasonable expectation of privacy. Perhaps people could be threatened or punished for their political commitments or their religion. Perhaps their conversations, or relevant "meta-data," could be released to the public, thus endangering domains that are, or have become, central to private life. Perhaps officials will see such conversations, or such meta-data, producing a degree of intrusion into the private domain.

There is also a risk to civil liberties, including freedom of speech; if government acquires meta-data, there might well be (or perhaps there now is) a chilling effect on free discussion, on journalists and on journalists' sources. Extensive forms of surveillance also create risks to commercial and economic interests and to relationships with foreign nations. Each of these risks could be elaborated in great detail. For now, we need not undertake the relevant elaboration; the underlying risks have received a great deal of attention and have helped animate proposals for reform.[27] The central point is that a form of Cheneyism, focused reasonably but solely on risks associated with terrorism, artificially truncates an appropriately wide viewscreen.[28]

B. Snowdenism

Focusing on an important subset of risks, some people embrace a Privacy Precautionary Principle. In their view, the risk to personal privacy requires political reforms that reduce the risk that an incompetent or ill-motivated government might, now or at some future time, jeopardize personal privacy. In one form, associated with Snowdenism, the objection is that some invasions of privacy have already occurred and are unacceptable in a free society. In another form, also associated with Snowdenism, the claim is that more egregious invasions are possible or likely, if corrective steps are not taken.

An evident source of the Privacy Precautionary Principle is the availability heuristic: To some people, certain highly publicized cases of abuse are highly salient, not least in

[26] See Report, supra note *, for a detailed discussion.
[27] See note * supra.
[28] It is true, of course, that one might endorse policies that are designed above all to reduce risks of terrorism, and that give little attention to privacy, civil liberties, and related values, not because of a limited viewscreen, but on the theory that a sensible approach to risk management, taking full account of the relevant values, justifies those policies. The discussion below is meant to address this conclusion.

the United States and Europe, and they make the risk of future abuse seem far from speculative. Another underpinning is loss aversion: People are used to certain safeguards against invasion into what they see as their private domain, and widespread surveillance threatens to impose significant losses to core interests in freedom, dignity, and civic respect. A final underpinning is probability neglect. It is easy to imagine (and in the view of some to identify) privacy violations of an extreme or intolerable sort,[29] and because those violations call up strong emotions, the very possibility that they will occur stirs strong emotions.

At the same time – and to return to my general theme -- a Privacy Precautionary Principle, taken by itself and for all that it is worth, would not make a great deal of sense, if only because it would give rise to national security risks, and potentially serious ones. The problem is that if our only or central goal is to eliminate any and all risks to privacy, we would abandon forms of surveillance that might turn out to save lives. Safeguards for privacy are of course exceedingly important, but at the conceptual level, the question remains: Why should a nation adopt a form of precautionary thinking in the context of privacy while repudiating it in the context of national security?

This question suggests that the relevant questions are best understood as involving a form of risk management. As in the environmental context, so too in the context of national security: Risks of many kinds are on both sides of the ledger, and the task is to manage the full set, not to focus on one or few. But the concept of risk management remains to be specified, and in the context of national security, the effort at specification creates serious challenges. Call this the *epistemic difficulty*, and it produces formidable problems for sensible risk management in this context.

III. Expected Values and Worst-Case Scenarios

A. The Epistemic Difficulty, Contextualized

Ideally, of course, we would be able to identify a range of possible outcomes, to assign probabilities to each, and to come up with some kind of common metric by which to make sensible comparisons. In regulatory policy in general, there is now a broad consensus in favor of cost-benefit analysis, understood as an effort to assess the benefits and costs of various options, and to weigh the two against each other.[30] Suppose, for example, that the monetized costs of an airline safety regulation are $400 million and that the monetized benefits are $70 million. If so, the regulation is unlikely to proceed, at least unless the law requires it, or unless nonquantifiable benefits can be invoked to tip the balance.[31]

One of the hardest challenges for cost-benefit analysis, of course, is that many of the variables at stake can difficult or perhaps even impossible to monetize, thus

[29] See the discussion in Report, note * supra.
[30] See Executive Order 13563; Cass R. Sunstein, Valuing Life (2013).
[31] See id.

producing one kind of epistemic difficulty.[32] In some of the most challenging cases, we might not be able to specify the relevant quantities even before we turn them into monetary equivalents. It might be unclear whether an air pollution regulation will save 500 lives, or 1000 lives, or 2000 lives, or 3000 lives. If the value of a statistical life is $9 million, then the monetized mortality benefits range from $4.5 billion to $27 billion – a stunningly wide range. And in some regulatory settings, benefits cannot be quantified in any helpful way, simply because regulators lack relevant knowledge. Here the epistemic difficulty turns out to be formidable.[33]

In the context of national security, the challenge of quantification can be even more daunting. Suppose that the relevant risk is a terrorist attack. In advance, it might be exceedingly difficult to quantify the costs of such an attack. How many lives are at risk? Ten? Two hundred? Three thousand? More? Even if the number is at the low end of the scale, we have seen that any terrorist attack has proliferating costs, some of them involving life itself.[34] Of course assessment of the expected value of precautions must also engage the question of probability: If initiative A is undertaken, what is the reduction in the probability of a successful terrorist attack? Officials might not be able to specify the answer to that question. In this respect, the domain of national security overlaps with that of financial regulation, where identification of the benefits of regulatory safeguards can also be daunting.[35]

There are second-order effects as well as first-order effects: What kinds of social consequences follow from a successful terrorist attack? Do they include long-term economic costs? Do they include intrusions on privacy and liberty? If so, how should these be counted in the risk management calculation? Should a civil libertarian favor national safeguards that appear to threaten civil liberties, on the ground that if they are successful, those very safeguards will help to preserve civil liberties against further intrusions? These questions might prove difficult to answer when policymakers are assessing particular programs.

B. Breakeven Analysis (and its Discontents)

Even if such questions do not have clear answers, officials may not be entirely at sea. Within the federal government, it is standard to speak of "breakeven analysis," by which officials ask: *What would the benefits have to be, in order for it to be worthwhile to impose the costs*[36]? Suppose, for example, that the costs of a rule that would protect against some environmental risk are $200 million, but the benefits cannot be specified.

[32] See Cass R. Sunstein, The Limits of Quantification, 102 Cal. L. Rev. 1369 (2014).

[33] See Coates, supra note.

[34] See Gerd Gigerenzer, Dread Risk, September 11, and Fatal Traffic Accidents, 15 Psych Science 286 (2004).

[35] See John Coates, Financial Regulation and Cost-Benefit Analysis, Yale LJ (2015).

[36] See Sunstein, supra note.

We might be able to say that at its upper bound, the cost of the environmental damage, if it were to occur, would be $100 million. If so, the rule could not easily be justified.[37]

Now suppose that at its upper bound, the cost of the environmental damage would be $900 million. If so, it is not clear that the benefits fail to justify the costs. An obvious question would be: What kind of contribution would the rule have to make to prevention of the damage? If the rule can be taken to reduce the risk by 10 percent, the benefits and the costs would be fairly close. Of course the agency might not be able to specify any such percentage. But perhaps it is able to identify lower and upper bounds. If the lower bound, in terms of risk reduction, is (say) 15 percent, then the benefits do seem to justify the costs.

With approaches of this kind, breakeven analysis can make seemingly intractable problems far more tractable. Suppose, for example, that officials know the upper or lower bound of costs associated with a risk, if it comes to fruition, or suppose that they know about the number of people or activities that might be affected (even if they do not know the costs of the per-person or per-activity impact). If so, breakeven analysis might prove feasible, and it might suggest that a regulation is either clearly desirable or clearly a mistake. Even in standard settings, it is possible that regulators will know too little to make use of that form of analysis, but if they have even small pockets of knowledge, the approach can greatly clarify their judgments.

At least in theory, breakeven analysis can play a role in the context of national security as well. There are many complexities here, so let us consider a highly stylized example. Suppose that the cost of a terrorist attack, if it were to occur, is at least $200 billion, and suppose that the measure in question would reduce the probability of its occurrence by 10 percent. (Nothing turns on these particular numbers, which are introduced simply for purposes of analysis.) Suppose too that the measure in question would consist of security precautions at airports or certain forms of surveillance. We might ask: Is the cost of an invasion of privacy in excess of $20 billion? Of course there is no purely arithmetic answer to that question,[38] but the question itself might turn out to be helpful, at least if we know something about the nature of the risk to privacy. Advocates of the measure will ask a legitimate question: Is it plausible to think that the risk to privacy is worth $20 billion?

This is of course an artificial example, and in this context, breakeven analysis runs into particular trouble, at least if we indulge the reasonable assumptions that a great deal of important information is missing, and that moral valuations will play an inescapable role. When hard-to-quantify costs are on both sides of the ledger – as they are in the contexts under discussion – then breakeven analysis becomes especially hard to

[37] For present purposes, I am putting to one side questions about distribution and equity, and also questions about nonquantifiable benefits. For relevant discussion, see id.

[38] I am putting to one side questions about the use of willingness to pay to value privacy issues.

undertake. If so, its chief advantage is that it may promote transparency about the issues involved.[39]

C. Avoid Gratuitous Costs

Diverse people should be willing to converge on a simple principle: *avoid gratuitous costs*. In the environmental context, that seemingly self-evident principle turns out to have real bite. Suppose, for example, that on reflection, certain environmental risks turn out to be de minimis, in the sense that they are trivial.[40] It makes sense to say that government should not regulate those risks, at least if regulation itself imposes costs. The principle is also important in the context of national security. Suppose that some forms of surveillance produce no benefits, or de minimis benefits. Suppose that their only function is to pick up information that cannot plausibly contribute to the prevention of terrorist attacks. If so, there would seem to be no reason that they should be continued.

The principle does not only inform the scope of surveillance activities. It should also inform the design of relevant institutions. For example, the President's Review Group recommended that meta-data should be held not by the government itself, but by the phone companies, with access by the government on the basis of the appropriate showing.[41] We can understand this recommendation as an outcome of the no-gratuitous-costs principle: On optimistic (but not unrealistic) assumptions, it would deprive the government of exactly nothing that it is important for the government to have, while also providing a layer of protection against risks to privacy and free speech. Even if the government does not "hold" the meta-data, it can obtain it on a showing of need, and indeed if time requires (for example, under emergency conditions), it need not obtain judicial authorization in advance.[42] Under these assumptions, the Review Group's recommendation flows directly from the no-gratuitous-harm principle.

That principle is a sensible way to provide a layer of privacy protection without threatening national security. A much more controversial question: Can the principle be used to *scale back* some kinds of apparent privacy protection, on the ground that they do no real good, in terms of privacy, but also impose some costs (in the form of national security risks)? However uncomfortable, the question deserves attention.

D. Avoiding Illicit Grounds

If the purpose of surveillance is to protect national security, then some grounds for surveillance, and some uses of surveillance, are automatically off-limits. They do not

[39] See Sunstein, The Limits of Quantification, supra note.
[40] In the easiest cases, the judgment of triviality comes from the fact that even if they come to fruition, they do not involve much harm. In harder cases, the judgment of triviality comes from a calculation of expected value. If such a calculation is possible, of course, then the epistemic difficulty is not so large.
[41] See note supra.
[42] See id.

count in the balance at all.[43] This is an exceedingly important idea, because it captures, and takes directly on board, some of the most plausible judgments behind a Privacy Precautionary Principle. More specifically, it addresses several concerns that motivate that principle.

The major categories are straightforward.[44] Surveillance cannot legitimately be used to punish people because of their political views or their religious convictions. Under current conditions, surveillance that is designed to reduce risks to national security should not be designed to protect against criminal activity that raises no national security issue.[45] If the underlying activity involves unlawful gambling or tax evasion, there are established routes by which government may obtain relevant information. It is generally agreed that surveillance should not be designed to give a commercial advantage to American firms. In these and other respects, the interest in national security – which is what motivates surveillance in this context -- also limits and disciplines the permissible grounds for surveillance. No sensible form of Cheneyism should reject those limits.

To be sure, we could imagine more difficult cases. Suppose, not implausibly, that a certain set of political views, or identifiable religious convictions, are closely associated with a desire to do harm to the United States and its allies. If people are members of the Islamic State of Iraq and the Levant (ISIL), the United States is entitled to focus on them by virtue of that fact. But the reason involves national security, not politics or religion as such. We can imagine cases that might test the clarity of that line, but the basic principle should not be obscure.

E. Avoid the Worst of the Worst Cases

Decision theorists sometimes distinguish between situations of risk, where probabilities can be assigned to various outcomes, and situations of uncertainty, where no such probabilities can be assigned.[46] In the domain of national security, we can imagine instances in which analysts cannot specify a usefully narrow range of probabilities, and in which the extent of the harm, from bad outcomes, is also not susceptible to anything like precise prediction. Here again, the analogy to financial regulation is plausible: Analysts might be able to identify only an unhelpfully wide range of bad outcomes, and they might not be able to say a great deal about the contribution of a regulation to prevention of such outcomes.[47]

[43] See the discussion of "exclusionary reasons" in Joseph Raz, Practical Reason and Norms (2d ed. 1990).

[44] See Report, supra note *.

[45] To be sure, there are imaginable complexities here, as where surveillance, meant to protect against national security risks, uncovers a plan to commit acts of violence that do not involve national security.

[46] Sere Frank H. Knight, Risk, Uncertainty, and Profit (1933); Paul Davidson, Is Probability Theory Relevant for Uncertainty? A Post-Keynesian Perspective, 13 Journal of Post-Keynesian Economics 129 (1991).

[47] Coates, supra note.

In situations of uncertainty, when existing knowledge does not permit regulators to assign probabilities to outcomes, it is standard to follow the maximin principle: *Choose the policy with the best worst-case outcome.*[48] Suppose that the worst case associated with one policy involves a successful terrorist attack on the United States, with consequently significant loss of life. Suppose that the worst case associated with another policy involves a serious threat to privacy, in the form (say) of widespread official reading of private meta-data (or more), leading to official invasion of the private sphere. Suppose finally that we cannot say much about the probability that one or another worst case will occur. In a case of that kind, there is a good argument for Cheneyism, and a much weaker one for Snowdenism. The reason is that the worst case associated with a successful terrorist attack is so much worse than the worst case associated with a breach of personal privacy.

Of course the case is artificial along multiple dimensions. We might be speaking of *bounded uncertainty*: In a particular period, the probability of a successful terrorist attack might not be between 0 percent and 100 percent, but between 0 percent and 30 percent (though we might not be able to say much about where it falls within that range). We might be able to say that if a terrorist attack occurs, very bad outcomes would have a cost between $X and $Y, where $X is (say) $100 billion, and where $Y is (say) $950 billion. (This numbers are merely illustrative.) And while the contribution of a particular contribution might not be susceptible to precise specification, policymakers might have an idea of a sensible range.

Moreover, maximin is most useful in cases where the outcomes can easily be rendered commensurable. Suppose that a policymaker has two options, which would lead to different worst-case scenarios: (1) a loss of $500 million or (2) a loss of $900 million. The option that leads to the lower worst-case loss is better (and it is clear which is lower). Or suppose that with option 1, the worst-case scenario involves a loss of 1000 lives, whereas with option 2, the worst-case scenario would lose 6000 lives (no ambiguity there). But the issue is more difficult when the outcomes are not easily made commensurable. Suppose that a policymaker has two options, with different worst-case scenarios: (1) a loss of $900 million and also 200 lives and (2) a loss of $600 million and also 150 lives. Are the 50 lives saved (from (2) worth the $300 million cost? The answer depends on the value of a statistical life. The government now values a statistical life at about $9 million, so the answer is yes.

But far harder cases are imaginable. In the context at hand, suppose that with one approach, the worst-case scenario is a loss of significant numbers of lives, whereas with another, the worst-case scenario is a massive intrusion into personal privacy. For progress to be made, both of these would have to be specified. How many lives? 1000, or 5000, or 40,000? More? And what kind of intrusion counts as massive? Issues of valuation cannot be avoided here. Official reading of (say) private meta-data is far more alarming to some people than to others. On one view, a certain degree of vulnerability, with respect to

[48] See Jon Elster, Explaining Technical Change 185-207 (1983), for a helpful discussion.

private meta-data, does not involve anything like the worst-case scenarios associated with successful terrorist attacks. That view might be accompanied by a judgment that the risk of vulnerability, with respect to private meta-data, can be sufficiently contained. But on another view, a cavalier approach to personal privacy threatens both liberty and self-government themselves, and so the worst-case scenario is very bad indeed (and cannot be ruled out).

Disagreements of this kind cannot be resolved by arithmetic. A reference to maximin will not do the trick. Perhaps the best that can be done is to attempt to identify safeguards, with respect to privacy, that plausibly reduce the risks associated with worst-case scenarios, will also allowing officials to do what must be done with respect to protect national security. In the abstract, it might well seem more difficult to achieve that goal that it is in practice.[49]

Conclusion

In ordinary life, people take precautions, and sensibly so; insurance policies are often an excellent idea. The Precautionary Principle is animated by the reasonable idea that it is prudent to act even when it is far from certain that the underlying danger will come to fruition. The problem is that action can create dangers of its own. In the environmental context, the Precautionary Principle runs into self-evident trouble when efforts to reduce some environmental risks give rise to other environmental risks. But it is also problematic when those efforts create risks that have nothing to do with the environment. A wide viewscreen, rather than a narrow one, is indispensable in the regulatory domain.

In the area of national security, it may be especially tempting for public officials to adopt some kind of Precautionary Principle, not least because they are confronted with a dazzling array of low-probability risks. It would be both irresponsible and dangerous to ignore those risks. At the same time, some precautions create risks of their own, and they must be considered in an overall balance. Cheneyism, as I have understood it here, runs afoul of the need for wide viewscreens. The same point certainly holds for those who embrace Snowdenism, which I have understood as an insistence on a Precautionary Principle for privacy and civil liberties.

To the extent feasible, the best approach to risk management involves cost-benefit balancing. The challenge is that in some domains, both costs and benefits are exceedingly hard to quantify, much less to monetize; the epistemic difficulty is severe, and breakeven analysis itself runs into formidable difficulties. I have argued for four ideas that can help. First, officials should consider the use of breakeven analysis. Second, they should not impose essentially gratuitous costs (including risks). Third, they should ensure that illicit grounds are not being invoked to intrude on privacy, liberty, or anything else. Fourth, they should take steps to prevent the worst of the worst-case scenarios. There are no algorithms here, but a form of risk management, embodying those ideas, can help to

[49] See Report, supra note.

avoid some of the pathologies of both Cheneyism and Snowdenism: Precautionary Principles of the most blinkered or myopic sorts.