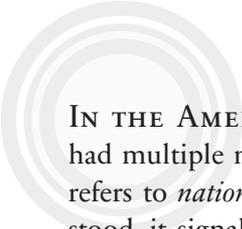


Chapter One

PRINCIPLES

1. The United States Government must protect, at once, two different forms of security: national security and personal privacy.



IN THE AMERICAN TRADITION, the word “security” has had multiple meanings. In contemporary parlance, it often refers to *national security* or *homeland security*. Thus understood, it signals the immense importance of counteracting threats that come from those who seek to do the nation and its citizens harm. One of the government’s most fundamental responsibilities is to protect this form of security, broadly understood. Appropriately conducted and properly disciplined, surveillance can help to eliminate important national security risks. It has helped to save lives in the past. It will help to do so in the future.

In the aftermath of the terrorist attacks of September 11, 2001, it should not be necessary to belabor this point. By

CHAPTER ONE

their very nature, terrorist attacks tend to involve covert, decentralized actors who participate in plots that may not be easy to identify or disrupt. Surveillance can protect, and has protected, against such plots. But protection of national security includes a series of additional goals, prominently including counter-intelligence and counter-proliferation. It also includes support for military operations. Amidst serious military conflicts, surveillance can be an indispensable means of protecting the lives of those who serve or fight for our nation, and also (and it is important to emphasize this point) for our friends and allies.

At the same time, the idea of security refers to a quite different and equally fundamental value, captured in the Fourth Amendment to the United States Constitution: “The right of the people to be *secure* in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated . . .” (emphasis added). This form of security is a central component of the right of privacy, which Supreme Court Justice Louis Brandeis famously described as “the right to be let alone—the most comprehensive of rights and the right most valued by civilized men.”¹ As Brandeis wrote, “The makers of our Constitution undertook to secure conditions favorable to the pursuit of happiness. They recognized the significance of man’s spiritual nature, of his feelings, and of his intellect. . . . They sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations.”²

This protection is indispensable to the protection of security, properly conceived. In a free society, one that is genuinely committed to self-government, people are secure in the sense that they need not fear that their conversations and activities are being watched, monitored, questioned, inter-

¹ *Olmstead v. United States*, 277 US 438, 478 (Brandeis, J., dissenting).

² *Id.*

rogated, or scrutinized. Citizens are free from this kind of fear. In unfree societies, by contrast, there is no right to be let alone, and people struggle to organize their lives to avoid the government's probing eye. The resulting unfreedom jeopardizes, all at once, individual liberty, self-government, economic growth, and basic ideals of citizenship.

It might seem puzzling, or a coincidence of language, that the word "security" embodies such different values. But the etymology of the word solves the puzzle; there is no coincidence here. In Latin, the word "securus" offers the core meanings, which include "free from care, quiet, easy," and also "tranquil; free from danger, safe." People who are at physical risk because of a threat of external violence are by definition in danger; they are not safe. So too, people made insecure by their own government, in their persons, houses, papers, and effects, can hardly be "free from care" or "tranquil." And indeed, the first sentence of the Constitution juxtaposes the two values, explicitly using the word "secure":

"We the People of the United States, in Order to form a more perfect Union, establish Justice, insure domestic Tranquility, *provide for the common defense*, promote the general Welfare, and *secure the Blessings of Liberty to ourselves and our Posterity*, do ordain and establish this Constitution for the United States of America" (emphasis added).

Some people believe that the two forms of security are in irreconcilable conflict with one another. They contend that in the modern era, with serious threats to the homeland and the rise of modern communications technologies, the nation must choose between them. We firmly reject this view. It is unsupported by the facts. It is inconsistent with our traditions

CHAPTER ONE

and our law. Free societies can and must take the necessary steps to protect national security, by enabling public officials to counteract and to anticipate genuine threats, while also ensuring that the people are secure “in their persons, houses, papers, and effects.”

2. The central task is one of risk management; multiple risks are involved, and all of them must be considered.

When public officials acquire information, they seek to reduce risks, above all risks to national security. If the government is able to obtain access to a great deal of information, it should be in a better position to mitigate serious threats of violence. And if the goal is to reduce such threats, a wide net seems far better than a narrow one, even if the government ends up acquiring a great deal of information that it does not need or want. As technologies evolve, it is becoming increasingly feasible to cast that wide net. In the future, the feasibility of pervasive surveillance will increase dramatically. From the standpoint of risk reduction, that prospect has real advantages.

The challenge, of course, is that multiple risks are involved. The government must consider all of those risks, not a subset, when it is creating sensible safeguards. In addition to reducing risks to national security, public officials must consider four other risks.

RISKS TO PRIVACY. It is self-evident that as more information is acquired, the risk to privacy increases as well. One reason is that officials might obtain personal or private information that has nothing to do with threats of violence or indeed with criminality at all. History shows that the acquisition of information can create risks of misuse and abuse, perhaps in the form of intrusion into a legitimately private sphere. His-

tory also shows that when government is engaged in surveillance, it can undermine public trust, and in that sense render its own citizens insecure. Privacy is a central aspect of liberty, and it must be safeguarded.

RISKS TO FREEDOM AND CIVIL LIBERTIES ON THE INTERNET AND ELSEWHERE. Liberty includes a range of values, such as freedom of speech, freedom of religion, and freedom of association, that go well beyond privacy. If people are fearful that their conversations are being monitored, expressions of doubt about or opposition to current policies and leaders may be chilled, and the democratic process itself may be compromised.

Along with many other nations, the United States has been committed to the preservation and expansion of the Internet as an open, global space for freedom of expression. The pursuit of Internet freedom represents the effort to protect human rights online. These rights include the right to speak out, to dissent, and to offer or receive information across national borders. Citizens ought to be able to enjoy these rights, free from fear that their words will result in punishment or threat. A particular concern involves preservation of the rights, and the security, of journalists and the press; their rights and their security are indispensable to self-government.

RISKS TO OUR RELATIONSHIPS WITH OTHER NATIONS. Insofar as the information comes from other nations—whether their leaders or their citizens—its acquisition, dissemination, or use might seriously compromise our relationships with those very nations. It is important to consider the potential effects of surveillance on these relationships and, in particular, on our close allies and others with whom we share

CHAPTER ONE

values, interests, or both. Unnecessary or excessive surveillance can create risks that outweigh any gain. Those who do not live within our borders should be treated with dignity and respect, and an absence of such treatment can create real risks.

RISKS TO TRADE AND COMMERCE, INCLUDING INTERNATIONAL COMMERCE. Free trade, including free communications, is important to commerce and economic growth. Surveillance and the acquisition of information might have harmful effects on commerce, especially if it discourages people—either citizens of the United States or others—from using certain communications providers. If the government is working closely or secretly with specific providers, and if such providers cannot assure their users that their communications are safe and secure, people might well look elsewhere. In principle, the economic damage could be severe.

These points make it abundantly clear that if officials can acquire information, it does not follow that they *should* do so. Indeed, the fact that officials can *legally* acquire information (under domestic law) does not mean that they should do so. In view of growing technological capacities, and the possibility (however remote) that acquired information might prove useful, it is tempting to think that such capacities should be used rather than ignored. The temptation should be resisted. Officials must consider all relevant risks, not merely one or a subset.

To this point we add an additional consideration, which is the immense importance of maintaining public trust. Some reforms are justified as improvements of the system of risk management. Other reforms are justified, not only or primarily on that ground, but as ways to promote a general sense, in the United States and abroad, that the nation's practices and decisions are worthy of trust.

3. The idea of “balancing” has an important element of truth, but it is also inadequate and misleading.

It is tempting to suggest that the underlying goal is to achieve the right “balance” between the two forms of security. The suggestion has an important element of truth. Some tradeoffs are inevitable; we shall explore the question of balance in some detail. But in critical respects, the suggestion is inadequate and misleading.

Some safeguards are not subject to balancing at all. In a free society, public officials should never engage in surveillance in order to punish their political enemies; to restrict freedom of speech or religion; to suppress legitimate criticism and dissent; to help their preferred companies or industries; to provide domestic companies with an unfair competitive advantage; or to benefit or burden members of groups defined in terms of religion, ethnicity, race, or gender. These prohibitions are foundational, and they apply both inside and outside our territorial borders.

The purposes of surveillance must be legitimate. If they are not, no amount of “balancing” can justify surveillance. For this reason, it is exceptionally important to create explicit prohibitions and safeguards, designed to reduce the risk that surveillance will ever be undertaken for illegitimate ends.

4. The government should base its decisions on a careful analysis of consequences, including both benefits and costs (to the extent feasible).

In many areas of policy, public officials are increasingly insistent on the need for careful analysis of the consequences of their decisions and on the importance of relying not on intuitions and anecdotes, but on evidence and data, including benefits and costs (to the extent feasible). In the context

CHAPTER ONE

of government regulation, President Ronald Reagan established a national commitment to careful analysis of regulations in his Executive Order 12291, issued in 1981. In 2011, President Barack Obama issued Executive Order 13563, which renewed and deepened the commitment to quantitative, evidence-based analysis, and added a number of additional requirements to improve regulatory review, directing agencies “to use the best available techniques to quantify anticipated present and future benefits and costs as accurately as possible” in order to achieve regulatory ends.

A central component of Executive Order 13563 involves “retrospective analysis,” meant to ensure not merely prospective analysis of (anticipated) costs and benefits, but also continuing efforts to explore what policies have actually achieved, or failed to achieve, in the real world. In our view, both prospective and retrospective analyses have important roles to play in the domain under discussion, though they also present distinctive challenges, above all because of limits in available knowledge and challenges in quantifying certain variables.

Before they are undertaken, surveillance decisions should depend (to the extent feasible) on a careful assessment of the anticipated consequences, including the full range of relevant risks. Such decisions should also be subject to continuing scrutiny, including retrospective analysis, to ensure that any errors are corrected.

As we have seen, there is always a possibility that acquisition of more information—whether in the US or abroad—might ultimately prove helpful. But that abstract possibility does not, by itself, provide a sufficient justification for acquiring more information. Because risk management is inevitably involved, the question is one of benefits and costs, which requires careful attention to the range of possible outcomes and also to the likelihood that they will actually occur. To the

extent feasible, such attention must be based on the available evidence.

Where evidence is unavailable, public officials must acknowledge the limits of what they know. In some cases, public officials are reasonably attempting to reduce risks that are not subject to specification or quantification in advance. In such cases, experience may turn out to be the best teacher; it may show that programs are not working well, and that the benefits and costs are different from what was anticipated. Continued learning and constant scrutiny, with close reference to the consequences, is necessary to safeguard both national security and personal privacy, and to ensure proper management of the full range of risks that are involved.

Finally, in constructing oversight and monitoring of intelligence agencies and particularly of surveillance, the US Government must take care to address perceptions of potential abuse, as well as any realities. To maintain and enhance the required level of public trust, especially careful oversight is advisable.