In many countries journalists report independently at their peril: speaking truth about power runs the risk of retaliation from criminals or state officials—and at times it can be hard to distinguish between the two.

In countries with a commitment to the rule of law, journalists have much less to fear over their livelihoods or physical safety, notwithstanding the astonishing specter of three senior staff members of the *Guardian* who were compelled to smash their own computers containing leaked documents under the watchful eyes of officials from one of the United Kingdom’s intelligence agencies. That theater illustrates more the futility of government intervention than its effectiveness—the documents had already been replicated to ProPublica and the *New York Times*. In the years since, the *Guardian* editors have been publicly venerated—not jailed.

There has been a more insidious, less lurid threat to independent journalism in such countries: a withering away of public respect for professional journalists and traditional media, which in its best moments aspired to values other than simply what garnered the most clicks. Of course, we should not rue the disappearance of consolidated mass media...
and its oracular voice. And if anything, such consolidation may be returning: companies like Facebook are playing to become the new global newsstands, not only hosting others’ material but indexing and directing traffic to it—when they feel so moved.

In the lead-up to the computer-smashing incident, the Guardian had offered to work with the British government to help secure the files that Edward Snowden leaked against further compromise, while its editors reviewed them for journalistic value in the public interest. The government should have taken up the offer. And it is not too late for some of the inevitable leaks to come. Post-Snowden, governments should be ready to deal with leaks and leakers in ways currently off-limits, drawn from how they negotiate with mainstream newspapers when stories grounded in classified information were slated for publication. Imagine if the U.S. government had offered Edward Snowden a secure server on which to place his files, with a genuine promise to maintain access for some agreed-upon journalists, despite the government’s straightforward view that the files were illegally compromised. In turn, Snowden would endeavor to delete all other copies, and the journalists would agree to a process for listening to and evaluating the government’s case for why particular draft stories drawn from the documents would unduly hurt public safety. Ultimately the journalists would bear responsibility for deciding what to do.

Such an arrangement recognizes that role assignment is one of the best ways for a system to self-balance. It’s why a person who is a successful prosecutor or defense attorney may act quite differently once becoming a judge, or an elected official, or the head of an agency. When we ask people to inhabit too many roles at once, to perform balancing within their own minds or as part of small groups with common incentives, sensitive decisions will not be made well. Meaningful participation by elected legislators in surveillance policy is important, along with searching judicial review. But perhaps it is not enough without also having a responsible, independent media in the frame.

In a democracy, a government program that cannot be successfully publicly defended—whether because it is ethically wrong, or contrary to the rule of law, or simply because it is out of step with what an informed citizenry would want—should not persist simply thanks to secrecy. The longer the truth takes to get out, the greater the likelihood of haphazard and ill-contextualized leaks about it, and the higher the cost of accounting
for it, once people do know. Policies and practices in the earnest pursuit of security, which understandably begin in urgency after an attack or compromise, should be disclosed by governments in general terms soon after—indeed, not even waiting for a freedom of information request. The specter of an elected representative taking to the well of the Senate to say, “If you only knew what I did, you would disapprove greatly,” while unable ethically to begin a discussion with his colleagues at large or the general public about what troubled him, is a strong signal that the system before Snowden had become too insular, with no escape valve for when prudential and ethical, if not legal, lines had been crossed.

We urgently need to buttress our independent media around the world, including those outlets and individuals not affiliated with large news organizations but who embrace journalistic values. These organizations and people must be able to work without intimidation, and without blanket surveillance. Surely some of the tactics described in this book for operational security by the media are helpful. But they are also actions that over time generate reactions of more intensive and intrusive surveillance. Ultimately, technological maneuvers are no substitute for strong (if arm’s-length) respect and understanding between governments and journalists of their respective roles. The enemies of freedom and security shared by journalists and democratic governments alike are those regimes that do not even aspire to cultivate the rule of law, and that may end up inheriting or reinventing the tools and practices of surveillance honed and defended elsewhere. In any event, intense secrecy punctuated by indiscriminate Exxon Valdez–size leaks is the worst of both worlds.

Any postscript to this thoughtful volume is, given how quickly circumstances are changing, really a foreword to what will come next. These essays show how reasonable people, inhabiting their roles across the spectrum, will disagree on the specifics while agreeing through the fact of their contributions that the right to express oneself through speech, writing, and journalism is essential. Discourse—persuasion based on facts and rigorous back-and-forth, rather than the raw exercise of power—remains civilization’s most precious, if at times elusive, coin.