FOREWORD

The intelligence instrument and American democracy, at times, are uncomfortable partners. This is reflected in what have become serial controversies over FBI access to the iPhones of terrorists and criminals. It is reflected in the public’s reaction to the Snowden leaks and ensuing debate over the government’s use of Sections 215 and 702 of PATRIOT Act to collect communications data and metadata. And, it is reflected in debates about the use of rendition and targeted killing as security tools.

This tension is not new, as Henry Stimson might note. It was manifest during the Church and Pike Committee hearings of the 1970s, which exposed, examined, and critiqued U.S. intelligence activities of the 1950s and 1960s, including assassination plots, covert activities to change or destabilize governments, and executive surveillance of Americans without warrants and in some cases without apparent probable cause. The result was a series of framework intelligence statutes and executive orders, the advent of the congressional intelligence committees, and a latent lingering suspicion about the use of the intelligence instrument at home and abroad.

The fundamental and underlying question during the Church era was much the same as it is during the Snowden era: What are the appropriate legal, ethical, and policy limits on the conduct of U.S. intelligence activities? That is the fundamental question this volume addresses.

But whereas the foundational question remains the same, the context is different. There are a number of distinct and in some cases competing trends in the post 9/11 era. To start, the scale of the intelligence challenge is different. The intelligence community must arguably contend with more threats today than during the Cold War, where the focus was inexorably and necessarily on the Soviet Union. Today, the intelligence community is expected to provide warning and respond to threats as diverse as those emanating from non-state terrorist actors, like ISIS and Al-Qaeda, rogue states like North Korea, as well as contend with the regional and global rivalries presented by states like China, Russia, and Iran. Moreover, these threats arrive in new domains such as cyber and space. Perhaps most important, these threats are potentially catastrophic or existential in a way that only the Soviet Union, and perhaps Maoist China, could have been during the Cold War.

The scale of information that is potentially available and the means of collecting it are also different than during the Cold War by orders of magnitude, or more precisely, by orders of rhino-bytes, a number followed by 26 zeroes. In short, in an era of Big Data the means, methods, and scope of collection are different. Moreover, in light of the threats, presidents and intelligence specialists will feel compelled, or should feel compelled, to reach to the limits of collection capability as well as to the limits of the law, whichever comes first. They would be irresponsible not to do so. The age of Big Data also changes the scope and complexion of
what Sherman Kent described as the importance of having the man in the loop—
to timely identify intelligence that is relevant and actionable. That makes a compi-
lation of laws an essential form of transparency, for a democracy it is an intelli-
gence playbook and not just a lawyer’s essential tool.

Sixteen years of continuous military and intelligence conflict has also resulted
in more intelligence programs, more secrets, and more scrutiny. The first phenom-
eron is reflected in the advent of additional intelligence disciplines and agencies,
most notably homeland security, as reflected by DHS and the Watch List system.
The second phenomenon is illustrated with reference to the growth in the number
of classified secrets, as documented by the Public Interest Declassification Board.
Scrutiny comes in the form of legislative, judicial, and executive oversight, but
also in the form of media, IO, and NGO inquiry.

Our collective sense of privacy as well as our sense of common purpose has
also changed. With only some exception, the Cold War, and in particular the So-
viet Union and KGB, offered a unifying purpose to intelligence activity. The pub-
lic might question a particular action, but rarely the necessity of having a robust
intelligence capability. Not everyone is as sure now, or at least as sure that the case
has been made. We want to be protected from terrorist attack, but not necessarily
at the risk of our privacy. We want both. Or more precisely, not everyone is per-
suaded that more security must come at the cost of less privacy.

This trend is entwined with an additional trend, a diminished respect for and
trust in the institutions of government. This is reflected in, among other places, the
public response to the Snowden leaks and the government’s collection of metadata.
The Foreign Intelligence Surveillance Court reviewed and authorized the program
no less than 35 times, which means the architecture of oversight worked, all three
branches of government were involved. But that was not the general public reac-
tion.

In short and in sum, in almost every quantitative category this intelligence era
is one of more—more risk, more threats, more capacity, more information, more
law, more scrutiny, and more skepticism.

Whether one is ambivalent about intelligence or not, it remains a critical tool,
arguably the critical tool in addressing 21st century security threats. Why is that?
First, intelligence is the critical ingredient in a preventative counterterrorism para-
digm. You cannot prevent what you cannot see or detect. And communications
intelligence and human intelligence are the critical sources of warning and detec-
tion within this paradigm. They are the only sources with realistic chance of de-
tecting a singular terrorist or a terrorist cell. Second, the ability to collect, analyze,
and use all source intelligence, to inform decision and provide warning, is our
greatest security advantage. We have always known this with respect to technical
means like satellites. But what the public has yet to appreciate is that in the iPhone
era where terrorist threats come from private actors the ability to collect and ana-
lyze Big Data, including metadata about communications, is a technical means as
vital as satellites were during the Cold War. No state has more capacity to collect,
analyze, and use this data than the United States. It deters as well as informs.
Third, intelligence is the means by which the U.S. government can address mul-
multiple and diverse threats at once, with finite resources, by knowing when and where to wisely allocate and shift its resources.

That makes intelligence critical to liberty and to democracy, for liberty depends on security. That is because those who feel physically threatened are more inclined to dispense with liberty, or at least the liberty of suspect persons or classes. Imagine the impact of a second 9/11 scale attack. Moreover, as Omar Bradley observed at the height of the Cold War, security and liberty are not rivals, they are partners.

What then is the answer to this tension between democracy and intelligence, or privacy and access?

The Constitution provides for both security and liberty, not a trade-off between the two. Moreover, many rights are absolute, like the First Amendment right to religion and a free press or the Sixth Amendment right to a jury trial. Other rights contemplate a weighing of factors, like due process and the Fourth Amendment protection against unreasonable government searches and seizures. Moreover, many security-liberty tensions are really liberty-liberty tensions. For example, rather than ask how much privacy is one prepared to forego to protect the security of civil aviation, one might ask how much privacy is one prepared to forego in order to protect the liberty interest of the passenger on the aircraft to life, to travel, and to engage in commerce. Where one stands on this position, as is often the case, may depend on where one sits at a moment in time, literally, at a computer screen typing or on a plane traveling.

The answer to having a robust intelligence capability in a democracy is transparency and law. Transparency implies a duty to acknowledge and explain the purpose, limits, and permits of intelligence, while keeping opaque specific targets and capabilities. One lesson learned from the Snowden leaks is that the American public will not support intelligence collection if they do not understand it. And, most people, including many public officials and judges, don’t understand what intelligence is and how it is used. One duty of the ABA Standing Committee on Law and National Security is to help bridge this gap.

Law is the other answer. A second lesson of the Snowden leaks is that we are past a point where the public trusts the government to do its job on faith. They want to see the law applied. Law serves three purposes. It provides the substantive authority to act, and thus by extension defines the limits to that same authority to act. Moreover, where the law is clear and it is clearly invoked, albeit often in secret, operators are more likely to take risk in achieving the policy or intelligence goal presented. Law is also a form of transparency. In light of the threats presented, if the law allows it, we are probably doing it. And if the law can be interpreted to allow it, we are probably doing it as well.

The law, as reflected in this compilation, also provides essential process. Good process, which means timely, contextual, and meaningful process, is essential because it allows officials to timely respond to threats and wisely allocate resources. It also addresses the pathologies of national security, which are particularly manifest with intelligence, like secrecy, speed, cognitive bias, and the tendency to reach beyond necessity for fear of falling short of need. Good process
gets there first and guides actors back from the edge of the law, while at the same time also helping to focus finite resources on real threats.

Third, law is an essential national security value. The humane treatment of detainees, for example, is a legal requirement and value. But it is also a national security value if one takes the view that the humane treatment and interrogation of detainees is more likely to lead to information, credible information, and defection than is harsh treatment. And where there are competing values, process allows these values to be adjudicated in a conscious and accountable manner aware of the long as well as short term consequences of acting or failing to act.

The key to security in a democracy is intelligence. In turn, the key to intelligence in a democracy is trust, trust that the intelligence instrument will be used to inform decision, prevent surprise, prevent attack, and predict the future so as to better plan and prepare for it, and not for other purposes. Transparency and law are the key to trust. This compilation represents a compelling presentation of both. Therefore is a critical resource not just to the specialist, but to all who value security, liberty, and law.

Judge James E. Baker  
Chair  
ABA Standing Committee on Law and National Security