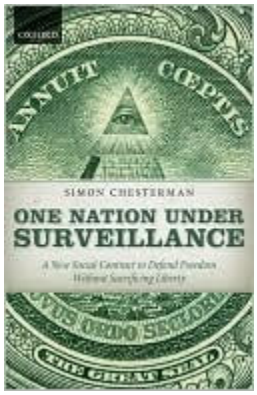
CARNEGIE COUNCIL
The Voice for Ethics in International Affairs

One Nation Under Surveillance: A New Social Contract to Defend Freedom Without Sacrificing Liberty

Simon Chesterman , Joanne J. Myers

March 22, 2011



One Nation Under Surveillance: A New Social Contract to Defend Freedom Without Sacrificing Liberty

Introduction

JOANNE MYERS: I'm Joanne Myers, and on behalf of the Carnegie Council I would like to thank you all for joining us this afternoon.

Simon is visiting from Singapore, where he is now based, and we are delighted to welcome him back to the Carnegie Council, this time to discuss a topic that concerns us all, our privacy.

His presentation is about how governments and other entities, especially since 9/11, are using our personal information under the rubric of national security concerns.

The act of balancing security concerns of the state with individual privacy has been around for some time. Even before the events of 9/11 and the release of WikiLeaks cables, a red flag about the issue of technological innovations and privacy had been raised when, in a 1963 Supreme Court opinion, Chief Justice Earl Warren observed that "the fantastic advances in the field of electronic communication constitute a great danger to the privacy of the individual."

The advances Chief Justice Warren alluded to have only accelerated since then. Simon writes that "in the past, spying on one's own citizens was subject to various restraints, but today threats from terrorists, advances in technology, and the amount of individual information we reveal about ourselves on the Internet have all led to a new environment, especially as warrantless electronic surveillance and government intercepts are on the rise. This leads many to argue that the very premise of privacy is under threat."

There have been quite a few debates over the appropriate responses to threats of violence and the need of the state to protect its citizens. In *One Nation Under Surveillance*, Simon examines many of these arguments. Still, if you are wondering about the limits—if any—that should be placed on a government's efforts to spy on its citizens in the name of national security, please note that Simon shifts the focus away from this line of questioning to ask whether and how governments should collect information, thereby moving the inquiry more toward the relevant questions concerning its use.

In doing so, he offers a framework which seeks to map out a new way of understanding intelligence-gathering in a modern context. This approach calls for a social contract between the privacy of the individual and the needs of the state.

Privacy matters. It is intrinsic to the concept of liberty. If we feel that we are being watched or listened to, we could lose our self-reliance and our sense of who we are, and free will along with our individuality.

Accordingly, Simon takes the debate into the 21st century as he clearly outlines mechanisms that will hold governments accountable.

Please join me in welcoming our guest today, Simon Chesterman. We're so happy to have you back.

Remarks

SIMON CHESTERMAN: Thank you very much indeed.

Next time I speak I want two people to precede me, one doing an advertisement and the other doing the small print, which was very helpful.

It's a great pleasure to be speaking at the Carnegie Council, an institution to which I routinely came to hear interesting speakers. I'm delighted to be invited here by Joanne and her colleagues to share with you some thoughts that are tangentially about privacy. It's partly about privacy, but in many ways my argument is essentially that the debates about privacy—well, you'll see. There are also elements of national security.

It's worth starting off by saying how I came to this issue, because I am by training an international lawyer. My interest in the area came when I was doing work at the International Peace Academy, which is now the International Peace Institute, on post-conflict reconstruction.

It was in the lead-up to the war with Iraq that I and many others—David Malone, many people—were shouting as loudly as we could, "Who's planning for post-conflict Iraq?" We obviously didn't do particularly well on that front.

The other thing that really began to interest me in that context was the way in which intelligence was being used in an international organization like the United Nations, most prominently Colin Powell's slide show at the UN Security Council to try and make the case for war with Iraq.

Eight years later, my research has taken me across various aspects of the way in which intelligence is used in intergovernmental organizations, and also to look at a couple of countries in particular.

What I'll do this evening is a speech in three acts.

- First, I'll talk about—and this is something Joanne touched on—the changing context. There are three trends that have really transformed debates about privacy from the type of literature that Joanne was citing in the 1960s; that means that the context in which we are evaluating these questions is radically different.
- Then I'll talk about three examples that I use in the book, the United States, the United Kingdom, and the United Nations—not so much case studies, but examples that tease out particular aspects of this debate.
- And then I'll try and wrap up with three lessons.

So it is three things of three.

Before I get started, another prefatory remark should be what I mean when I use a term like "intelligence." I teach a course in Singapore on intelligence law. One of the things I very quickly have to establish with the students is what intelligence is and what it is not.

Broadly, intelligence, at least as I'll use it today, can be understood in two broad contexts. The first is the collection of information obtained covertly—that is, sometimes referred to as "secret intelligence"—and the types of categories that have remained unchanged since the Second World War. Signals intelligence or, SIGINT (that is, what you write in your emails, say into your telephone, the transactions you engage in with your bank), and human intelligence—what I can trick, coerce, bribe, blackmail, and persuade you into telling me, or someone like me. You could add imagery intelligence or satellite photos as a more recent phenomenon. That's one sense in which intelligence is used as a kind of activity, of collecting information.

A second sense is intelligence in the sense of analysis, the product of intelligence services—a kind of "risk assessment intended to guide action" is how Michael Herman defined it. That's the product of intelligence services.

These are quite different functions; collection as opposed to analysis. One way of understanding this is to think of secrets as opposed to mysteries. An intelligence service might try and address both.

A secret might be, for example, how many nuclear weapons does Iran have. There is an answer to that question. It is a knowable fact. It might be difficult to find out the answer, but the answer is there.

A different question is what Mahmoud Ahmadinejad will do if Israel engages in certain foreign policy actions, or if the United States does something, or if there is certain unrest in Iran. That's not a knowable fact. Ahmadinejad himself might not know how he would respond. That's a mystery.

I'll be talking primarily about the collection side and focusing on the collapse of a traditional division in what intelligence services have been able to collect, because historically the collection of information, intelligence gathering on foreigners, has been regarded as an unseemly but necessary task, something that we really had to do. We didn't necessarily like it.

The laws of war are quite interesting on this front. Spying and the running of spies is lawful under the laws of war. But so is capturing, punishing, and executing spies if they are caught. So the spying on foreigners has long been accepted.

Spying on one's own citizens, at least in democracies, has been regarded with much greater suspicion and historically been subject to various forms of domestic legal and political restraint. In Western governments, this is also reflected not only in the law but in the organization—in the United States, the FBI has an internal mandate, the CIA an external mandate; in Britain, MI5 is internal and MI6 is external**.**

There have been grotesque violations of these principles—in the United States context, spectacularly culminating in the Watergate episode, which led to a reining in of intelligence services on the domestic front. But that scandal merely reinforced the view that foreign and domestic intelligence should and could be kept separate.

It is no longer tenable for three reasons. The first is that the threats have changed. In the book, I use a kind of flippant example to illustrate this, which is the story of Oleg Kalugin, who in 1958 came to Columbia University—not NYU, I should add, where I am still affiliated—where he studied as a journalism student, but at the same time was a young KGB agent who came to be promoted as the youngest general in its history.

Leap forward to the 1980s. Another guy was David Major, who was a career FBI agent and a counterterrorism advisor in the Reagan White House, whose job was to identify, track, and, if possible, turn in people like Kalugin.

They never met until the end of the Cold War, at which point both countries were downsizing their intelligence services. In the U.S. context, the proportion of the budget directed at the Soviet Union, or Russia, subsequently dropped from about 75 percent of the budget to about 16 percent. So a lot of guys were out of work.

David Major and Oleg Kalugin met up, and as enterprising fellows they started running a tourism service. You could take a bus ride for $35 a head with these guys giving you a blow-by-blow account of the dead-drop locations around Washington. Now you can do spy cruises with them as well. They have branched out.

That's a flippant example of what we are no longer focusing on. We are not focusing on what a major foreign power, like the Soviet Union, is doing.

The more troubling example is that the threats that have replaced this, in particular terrorism, no longer respect national borders and are not identifiable with a foreign power that could be plausibly deterred, and this therefore requires governments to address more and more of their intelligence-gathering powers domestically.

It is important not to overstate this threat. In the last four decades, the number of Americans who have been killed by terrorism is smaller than the number of Americans who have died as a result of lightning strikes or allergic reactions to peanuts. But, nonetheless, the most significant threat of violence on American soil is, and for the foreseeable future will remain, terrorism—not normally, it seems at the moment, state-sponsored terrorism, although maybe we could talk about what will happen in response to the ongoing situation in Libya in the question-and-answer.

The uncontroversial observation of the first trend is that the threats have changed.

The second trend that is changing intelligence-gathering is technology. Governments and many corporations have access to far greater technology to gather information on our populations, such as intercepted telecommunications and satellite photographs.

I was talking recently with people from the U.S. intelligence services who were observing that in the 1980s the most closely held of the secrets were satellite images, which you can now get freely available online through Google at as high resolution as you could in the 1980s.

In particular, I look at the rise of closed-circuit television in Britain, although soon I would guess, it is likely to be overtaken in New York. It has already been overtaken in Chicago. There is also the issue of DNA samples and biometric identification.

The technology that is available to governments to gather information has been growing exponentially, as has the capacity to store and analyze that information, which is no less important.

An example of the analysis is the E-ZPass in the United States, where you have to slow down to jogging pace so that the unit in your car can be read. In Singapore, where I live, you don't need to slow down but you still need an in-vehicle unit. In Britain, when they rolled out the congestion charge, no one needed to do anything; they just set up cameras that were smart enough to identify and record the license plate numbers of every vehicle going into and out of London. I was told recently that there are similar capacities in at least a couple of the tunnels coming into Manhattan.

So again, a pretty uncontroversial observation, that technology has also changed, which then enables greater surveillance.

The third trend, and in some ways the most interesting one to me, is that culturally we seem to be comfortable with all of this. We routinely use media in which we have no reasonable expectation of privacy.

I am old enough to have handwritten letters that I would have been outraged to find out had been steamed open and read. If you bother to read your end-use license agreements, every email you send, almost certainly your employer has access to. It's being filtered for spam or obscenities, and potentially it's being filtered for advertising purposes if you use Gmail. So you know, whether or not you act on this, that you don't have a significant level of privacy.

We draw irrational lines when we try to defend our privacy. Last year in Britain's general election, the national ID card became a major issue. It wasn't the decisive issue, but it was a major one in the Tories' campaign, and subsequently they followed through on a promise to abolish it.

But, interestingly, the reasons not to have an ID card in Britain had very little to do with traditional notions of what we might call privacy. Rather, the three issues that really got traction were the expense concern; worries about government competence in managing the data, because there had been some scandals on that front; and, thirdly, a kind of concern that the whole enterprise looked a little bit too "European," the idea of walking around with your papers.

It was also an odd situation to have Britain drawing this line on ID cards when London remains the CCTV capital of the world, and Britain as a country retains a database which has DNA samples of 10 percent of the population. That includes people who are convicted and go to prison for felonies, but also people who are detained on suspicion of felonies and have DNA samples collected and stored. This has been the subject of litigation in the European courts which is still ongoing.

In the United States, in the aftermath of September 11, there were occasionally somewhat irrational arguments about what gained traction as an issue. Some of you may remember, the librarians who started burning the borrowing records of patrons so that they wouldn't have to hand them over to the oppressive government, all to the credit of the librarians perhaps. But this was at the same time that thousands of people were being detained on immigration violations, warrantless electronic surveillance hadn't yet hit the news, and the United States was engaging in so-called enhanced interrogation, what we now call torture, in various black sites around the world.

As individuals, though, we are not much more rational than the societies that I have been describing. Many of you have Facebook accounts and routinely upload information onto social media sites that on reflection we might not if we were really worried about privacy.

This is not limited to my students and to dilettante academics like me who maintain Facebook accounts. I'll happily "friend" all of you if you approach me.

The wife of the current head of MI6, Britain's equivalent of the CIA, John Sawers' wife, had a Facebook account recently taken down, which included among other things the location of their London flat, the identity and whereabouts of their three children, and various other bits of information, including a somewhat amusing routine of her and her daughter doing a Liza Minnelli dance, and a picture of the current head of MI6 as a not-so-secret Santa, which was somewhat amusing.

These anecdotal examples are reflective of larger trends. Writing in the 1950s, after the McCarthy period, Edward Shils, a sociologist in the United States, said that liberal democracy, to function effectively, depended on maintaining privacy of individuals and denying privacy to government. In the following half-century exactly the opposite has happened: individual privacy has been eviscerated—or, I would argue, really given up—and governments have become ever more secretive.

In the 1990s, the nature of this debate can be illustrated by a fairly simplistic survey of the literature. There were two significant books in the 1990s with the words "Big Brother" in the title. Both were apocalyptic warnings of the coming surveillance state.

In the first decade of the 2000s, there were also two books with "Big Brother" in the title, both celebrating the reality TV program of the same name.

We aren't particularly rational in the way in which we think about these issues, and we tend to be extremely reactive, depending on how an issue is presented in the media. In recent years, the types of debates that have motivated us have been, in the United States context, warrantless electronic surveillance, which Joanne mentioned; ID cards in Britain. In coming years we'll have debates, almost certainly, about DNA databases, data mining, and biometric identification. There will be protests, lawsuits, editorials, and elections on these issues. These are all important battles.

I am at least assuming that the war is going to be lost, because these debates on the collection of information are doomed to failure. They are doomed because the modern threats that we are facing increasingly require governments to collect information on us. Governments are increasingly able to collect that information on us—that's the technological angle, and we as citizens increasingly accept, or at least tacitly accept, that they will collect that information.

In the book I'm not really saying that this is good or bad. I am saying, however, that it appears to be inevitable given the trajectory of government surveillance powers, but it is also linked in with the idea of what we now consider to be a modern and globalized life.

What I am trying to do is shift the debate away from whether or not governments should collect this information—it will be collected—and onto how that information should be used.

This brings me to the second part of my presentation, which is the three examples which I use, partly because they are interesting in their own right, but also because they bring out some larger lessons in this area.

The first, and the most important, is the United States. Although I have a picture from the U.S. one-dollar bill on the cover of my book, the audience is intended to be global.

The United States is the most important actor in this area. In some ways it's also the most transparent. But it has been no less reactionary in its response to threats than any other jurisdiction, perhaps even more so.

You can see, just tracking the efforts to impose oversight and regulation on the intelligence services, the reaction to major scandals. Very simplistically, Pearl Harbor and the aftermath of the Second World War led to a massive expansion in the intelligence capacity; Watergate—the scandals in that context led to a massive reining in of what came to be called the "rogue elephants" in the context of the Church and Pike committees; and then, after September 11, you again have the perception that "we've been restraining the power and the resources available to our intelligence services too much," and you have a massive expansion once again.

Two troubling themes have dominated or characterized the U.S. response to these new threats, in particular over the past decade, although some of the tendencies were already there.

The first, which has been widely commented on, is the abandoning of values and laws that the United States had done more than most to promote—the Geneva Conventions, the prohibition against torture, and domestic constraints on intelligence gathering. I won't belabor this point.

In popular culture, it came to be characterized by images like Jack Bauer in *24*, the Kiefer Sutherland pseudo-real-time series, which was interesting partly for the way in which it presented these issues and partly for the number of Homeland Security and intelligence officials I know who love the program. They love it both because it's very well made and it's exciting; but they also love the fact that members of the public think that's what their life is like. It's not at all like that. Most intelligence officials are essentially bureaucrats.

Soon, however, that kind of popular culture was overtaken by the very real horrors of Abu Ghraib. It is telling that in the aftermath of Abu Ghraib the only investigations and prosecutions were driven by photographs that had been released publicly. This is why it was primarily very low-level people were prosecuted in that context. That has been widely commented on. I'm not going to belabor that.

The second theme is the reliance on private contractors. This is distinct from the outsourcing phenomenon, the outsourcing of torture to Jordan, Syria, Egypt, and so on. What has been particularly striking is the reliance on private contractors for a growing proportion of the U.S. intelligence budget, and also in terms of the personnel involved.

Why is this a problem? In the U.S. context, outsourcing is embraced much more warmly by the government than in many other jurisdictions. Some of the work that I have done, and others in the room I know have done, on private military security companies illustrate the reasons to be concerned about such a trend towards outsourcing.

Among other things, the potentially abusive powers that are being exercised in our name by, if not employees, then delegates of the government, are being exercised by actors outside of traditional chains of command. That's a problem in the context of private military security companies, and also in intelligence.

For intelligence in particular, these powers are being exercised with express or implied immunity from legal process and in an environment precisely designed to avoid scrutiny. In particular, there have been arguments, which have gained a little bit of traction, on the dangers of outsourcing interrogation to private contractors. That is probably a line on which we might come to some agreement on stopping.

A more recent example shows other types of dangers of this outsourcing. It comes from a story that *The New York Times* at least released on Thursday, about a company called RSA, which manufactures fobs, or dongles, as they are sometimes called. These are two-factor authentication things that you use if you have a fairly high level of security, either on your bank, in your corporation, or if you're a government employee. You have a user name, a passport, and this little device. When you press a button, it gives you a six-digit number. RSA makes these for a bunch of corporations. They also make it for the NSA and the CIA.

On Thursday they revealed that they had been compromised by what is believed to have been a Chinese-organized hack. What's telling about the implications of privatization is that they had sat on this for a week. They had had internal meetings of the board trying to work out what this was going to do to their share price. They were in the process of acquiring a company, and so what was it going to do to that acquisition? Did they really need to release this to the public? What did they have to release and when?

It was only when really prompted, as far as I'm aware now, that they first went to the CIA and the NSA and then went public with this. You can imagine if it was a government agency—there are all sorts of reasons to be wary of government agencies having their own powers—but the debate would not have been about share price.

There is hope for change in both these areas, both in terms of the abuse of law or the misuse of law and the circumvention of law.

On the second day of his administration, President Obama announced that he would close Guantanamo Bay, end the CIA's secret prison program, and renounce torture. Yet, Guantanamo Bay not only remains in operation, it appears to have had a new lease on life recently. The apparent closure of secret prisons has not slowed the growth of the detention facility outside Bagram airfield near Kabul. And there have been very few meaningful investigations of the at least 100 deaths, 34 of which the U.S. military itself regarded as homicide deaths, in U.S. custody.

There does appear to be some movement on outsourcing. I mentioned the possibility of drawing a line at interrogations, which are regarded as an inherently governmental task. The primary issue that appears to be getting some traction on stopping outsourcing, is not that no one should be torturing or that only government employees should be torturing; it appears to be that these contract torturers cost twice as much as government employees.

So that is the United States. It is interesting partly for the departure from law and also the efforts to circumvent law.

Britain is interesting because for a long time it lacked laws completely in this area. MI5 and MI6 recently celebrated their centenary histories. For most of that history they had no legal framework whatsoever.

MI5 operated for most of the 20th century on the basis of a six-paragraph letter—interestingly, Mossad continues to operate on the basis of a three-paragraph letter from an Israeli prime minister.

Until 1992, the formal British position was that MI6, the secret intelligence service, did not exist. This wasn't a particularly well-kept secret, as by 1992 there had been 16 *James Bond* films. But nonetheless the official position was that MI6 did not exist and that its agents had no special powers.

Indeed, Lord Denning, known and beloved to common law students around the world, in the 1960s famously said that the members of the security service MI5 were "ordinary citizens." In an important sense this was true. They had no special powers, no immunities, and no warrants to give them special powers. They had to rely on not being caught, which for the most part they did, or prosecutorial discretion to make cases go away.

It was only as the result of European Convention on Human Rights litigation during the late 1970s and the 1980s that we saw Britain move their intelligence services onto a legislative footing, only really beginning in the 1980s, with the equivalent of their signals intelligence in 1995, the equivalent of the FBI in 1989, and the equivalent of the CIA in 1994.

I'm a lawyer, and you would think that putting these powers and agencies on a legislative footing would be a good thing. This includes Mr. Bond's license to kill. If you're interested, refer to Section 7 of the Intelligence Services Act of 1994. There are limitations to what the law can do if laws are drafted badly or too late.

On the badly drafted front, one of the fascinating things in Britain, going back to this idea of them as ordinary citizens, is that the formalization of these powers actually led to a massive expansion in their use.

The more recent legislation, 2000 Regulation of Investigatory Powers Act, when that was adopted there were eight agencies using these powers, mostly MI5 and MI6. In a couple of years, this expanded to 800 agencies, including local authorities.

In one notorious case that tellingly was broken by *The New York Times*, not by an English newspaper, council officials in Dorset trailed for three weeks and obtained the telephone records of Jenny Paton. Her alleged crime, which was later proved completely unfounded, that led to the breathless accounts of following the woman in her target vehicle with her three children, was that she was alleged falsely to have falsified her address in order to get her daughter into a good school. This is New York and I know it's hard to get into a good school, but for the surveillance powers of the state to be deployed, that at least seems to be an overreaction.

That is one example of perhaps badly drafted laws.

A related problem, which I won't touch on although we could talk about in discussion if you are interested, is if laws are drafted too late, it may not be possible to have a meaningful impact on the deployment of the surveillance powers of the state.

If you walk around London, just look at the number of CCTV cameras. The vast majority of these had been deployed and three-quarters of the crime-prevention budget was already being spent on closed-circuit TV cameras before the Human Rights Act came into force in 2000. It remains essentially unregulated as an area of practice in the United Kingdom. With the London Olympics coming up in 2012, London authorities actually sent people to Beijing to find out how to deploy CCTV even more effectively.

The third example which I will touch on is the United Nations, an issue familiar to many people in the room.

In 1993, Boutros Boutros-Ghali gave us a textbook example of a gaffe, which in American political life is when you accidentally speak the truth. What he said was that "the United Nations has no intelligence." [Laughter]

What he meant is that the UN doesn't have the capacity to collect secret information or a meaningful way to analyze information that it has. There have been various efforts throughout the history of the UN to develop this capacity, and usually it has been shut down either before it started or very soon after it began by Member States.

The International Peace Academy, the organization for which I and Sebastian von Einsiedel and others used to work, published a handbook in 1984, *The Peacekeeper's Handbook*, which literally said, "Intelligence is a dirty word."

You don't use intelligence in the context of the UN. You use words like "military information." If you look at the 2008 Capstone document, it looks like someone has gone through with a word processor just to replace "intelligence" with "information." Instead of "all sources intelligence" you have "all sources information," which doesn't make much sense.

As I mentioned at the beginning, I got interested in this whole area by the way in which intelligence was being used in the lead-up to the Iraq War.

Colin Powell's slideshow, which as we now know was based, at least in part, on fabricated intelligence from interested Iraqi informants, was nonetheless accepted by credulous American officials. Although it does bear repeating that Hans Blix and others believed that Iraq did have some kind of rudimentary weapons of mass destruction capacity, at least in the biological sphere.

There are plenty of other examples of the way in which intelligence posed problems in the United Nations.

Perhaps the issue that has seen a little bit of change recently is targeted financial sanctions, where individuals have their assets frozen worldwide on the say-so of one Member State, with no meaningful recourse to challenge that. In mid last year, an ombudsperson institution was set up, but this is the subject of ongoing litigation in the European courts. About a year ago in Britain, the implementing legislation was struck down and has led to all sorts of problems.

One issue is the accountability issue.

A second issue is the capacity to know what you are being given. Member States through most of the history of the United Nations tended to regard the United Nations more as a source of information rather than as a body with which you would share information, and when they do share it, usually it's for a purpose.

This is true most prominently in the freezing of assets, transparently in the lead-up to the war with Iraq in 2003, but even in areas like international criminal prosecution, where when Richard Goldstone started investigating the war crimes in the former Yugoslavia, he had no police force on the ground and no investigative capacity, but it was a war zone and there were plenty of foreign powers with an interest in having people like Karadžic and Milosevic indicted. There was a steady stream of information.

In the investigations phase this is incredibly useful, until you start to build a case to present in court and realize you can't use any of this. It presented all sorts of problems in the United Nations.

There are concerns that relate to the problem of having access to intelligence if you don't have experience in the area. That is true in the United Nations and for public officials when they first have access to intelligence—and indeed, academics like me.

When you first dip your toes into the intelligence world, there is a real danger that you start misinterpreting things and that you start seeing words like "top secret" as meaning true, whereas "top secret" just means it would be very damaging if it got out; it doesn't necessarily mean that it is true.

Or that you undervalue open-source information. A telling example of that is—and kudos to all the think-tank people in the room—Australian intelligence officials, even very senior ones, who are intensely interested in Indonesia and a group called Jemaah Islamiah in Indonesia, will confess that the best intelligence that they get on Jemaah Islahmiah comes not from Australian or American intelligence services; it comes from the International Crisis Group, because Sidney Jones on the ground knows everyone, does the work, does the best analysis, and produces the most useful result. I used to work for International Crisis Group, so I have an interest in this. But it's a telling example of how easy it is to overestimate the importance of intelligence and how dangerous it is to be seduced by it.

Those are the three examples. All of this is a provocation to conversation. In the last part of my presentation I'll try and tease out three lessons. I use these examples—the United States, Britain, the United Nations—to try and draw out some broader themes:

- The United States, to make an argument that these extraordinary powers that we give the government, which go beyond what corporations are able to do, at least able to do lawfully—the United States is an example of how those powers should be exercised by public authorities;
- Britain as an example of how those powers need to be grounded in the rule of law—but not just any law; and
- The United Nations as an example of how, if we are serious about guarding against misuse and abuse, we need to focus not just on collection but in particular on the use, not only by the body that collects that information, but also anyone with whom it is shared. I develop in the book a framework for trying to elaborate this, which I do through the vehicle of a social contract.

An example of how not to think about this was presented by Barack Obama in his inauguration speech in January 2009, where he sought to draw a line between this administration and the Bush Administration. He said: "We reject as false the choice between our safety and our ideals." It is important to emphasize that is absolutely true; it is false to suggest that there is a choice between safety and ideals. But nonetheless, the enduring convictions, of which he went on to speak in that inauguration, do change over time.

The new threats posed by terrorism, the opportunities offered by technological innovation, the acceptance of a public willing to compromise its privacy, have changed the context within which such decisions on national security matters are made, for although it is not either safety or ideals, decisions must still be made.

I try to look at this through a new form of an old idea, which is the social contract—in part, because it is a term routinely invoked, albeit it in fairly imprecise terms, by the intelligence community itself.

Michael Hayden, who is the previous director of the CIA, used this idea of a social contract in the hearings that had him confirmed. But he limited the meaning of the social contract to saying that all it really meant is that the CIA should obey the law and should maintain the trust of the American people.

Trust is important, but that doesn't imply a contractual relationship; it implies a fiduciary relationship. A fiduciary relationship in law is where one party, typically in a position of vulnerability, puts its faith in another to act on its behalf. You can imagine how that resonates with at least some in the intelligence world.

A contract, by contrast, implies an agreement negotiated by two parties.

The social contract has a long history in political theory. At its base it means that coercive political authority can be legitimized through some kind of pact—this is not an actual agreement that you sign, and that is one of the standard critiques of the contract area in theory—but that political association based on a measure of reasoned consent is both more legitimate and effective than other forms of political association.

For Thomas Hobbes, who wrote about this famously in *The Leviathan* in the 17th century, he was talking about the centralization of political authority that made organized society possible. To break free of the war of all against all, you needed to give power to the central authority, the Leviathan; otherwise life was going to be nasty, brutish, and short.

Today what I'm talking about is not this ceding of powers to a centralized authority—ceding powers like the monopoly over legitimate use of force, the ability to levy taxes, and so on. What I am talking about is ceding access to information in exchange for a measure of increased security and the conveniences of living in the modern world.

In this context, viewed through this kind of lens, I don't think privacy that Joanne was speaking about at the beginning is being stolen or ripped from us. We are giving it in exchange for these benefits. It's true that we often give it without much reflection, but the vast majority of the population appears to accept this transfer in practice.

There are differences from the traditional model of a social contract, in that here, at least in theory, you can opt out. You aren't compelled to have a mobile phone, an email address, use a credit card, get a driver's license, or fly. You probably can't stop a modern government knowing about your birth, income, and death, but apart from that it is possible to go off the grid. Few people choose this path, but it is a real choice. Alternatively, you can pay for anonymizing services and can mask your tracks.

It was striking that in 1998, there was a European Parliamentary report that basically said the United States and Britain, through the NSA and GCHQ [UK Government Communications Headquarters] can, and routinely do, intercept all telecommunications across Europe; every email, fax, and telephone call, the United States could be listening.

The response was not to protest and try and stop this. The response was to invest millions of euros in secure quantum cryptography, to try and develop practical responses—and this is what the United States does also.

It is possible to opt out. It's very hard, though.

The market for these types of products is growing. But privacy theorists have really struggled in this environment. Jonathan Franzen had a wonderful pithy summary of what privacy is and is not, because it's so hard to actually pin down what we mean by it, saying that privacy is "the Cheshire Cat of values, a very winning smile but not much substance," which is a useful metaphor to keep in mind.

Privacy theorists have really struggled to respond to all these moves, in part because of the diminishing sphere of truly private activity, and also the expanding coercive powers of the state.

A more fundamental problem might be that we continue to conceive the question as how to maintain a distinction between what is public and what is private. Here again, a contract area and analysis might be helpful—not in trying to protect that ever-diminishing sphere of what is private, but in recasting the debate as a dynamic relationship between government and governed.

Existing rules have been inadequate to this task and so new rules are required. The precise content of those rules will depend on the politics and the culture of the society in question, but it's possible to draw out some general principles that should apply across jurisdictions. These are three:

The first, and fundamental to the consensual premise of a contract, is that intelligence powers exercised must be public. The era of entirely secret agencies appears to be past. It's much harder to maintain the existence of a large secret agency, the way the NSA used to be the "no such agency" until the 1970s. Even in Singapore, the equivalent of the CIA, the Security and Intelligence Division, there's not a lot written up about them, but if you search the Ministry of Defence website you will at least find—in fact, the only reference you will find is how to say "Security and Intelligence Division" in Chinese. There's nothing else about it.

Its larger sense of publicness is not just about the existence of agencies, but that claims of national security made in our name are most credibly made by entities accountable to the nation. Outsourcing such responsibilities to private actors both undermines the legitimacy of the action and perverts the incentives that are intended to deter abuse.

This requirement of publicness would also acknowledge that the limits on those powers, what is acceptable and is not acceptable in our name, should be fought over in the political process rather than as part of an outsourced contract with a private entity.

Secondly, and implied by the notion of a formalized agreement, a contract, the entities carrying out these functions must be legal. Every agency's existence, mandates, and powers, must be established by law.

There must be limits for officers working in an intelligence agency, as well as limits to guide the politicians to whom they report. This is an important dual distinction. The legal mandate of an agency is not only to tell the agents what they are allowed to do and what they are not allowed to do; it's also a defense for them against the government perverting them to be used for other purposes, which in particular in Britain has been a historic dilemma, and to some extent the FBI under Hoover was an example of this.

Threats will continue to drive the Executive to push at the boundaries of law in its efforts to safeguard the nation. In some cases, the Executive might break the law. The rule of law can survive a breach; however, it probably cannot survive an entity that sits itself above the rule of law completely.

In addition to being public and legal, the third principle is going to the purpose of the contract, that accountability must be consequence-sensitive. Accountability as we currently understand it tends to be understood through examples such as a warrant-based system of individualized searches, which historically has been the primary mechanism in the United States, especially things like the Foreign Intelligence Surveillance Act and wiretaps locally.

This is largely irrelevant in an era of systematic surveillance of entire populations, or at least it's impractical. The focus instead needs to be on what is done with the information gathered.

Historically, efforts to deter or prevent abuse have focused on minimization protocols to reduce acquisition, limit retention of data, and constrain dissemination of that data. Systematic surveillance and our expanding storage capacities have reduced the significance of the first two elements—acquisition and retention. You can acquire much more and hold onto it for much longer periods in a big database. All three narrowly assume that the purpose of accountability is simply to deter or respond to abuse rather than to shape behavior in a more positive way.

There will be abuse, of course. Identities will be stolen, CCTV footage will be uploaded onto YouTube, and personal information will be lost.

There will also be discrimination. The most prominent example of this, implicit in the very notion of systematic surveillance, is profiling. As systematic surveillance and the capacity for data retention and analysis expand, it's possible that we might see an alternative to profiling. Rather than targeting a specific group for closer examination, it might be possible to gather information on the entire population in such depth that human intervention, with the subjectivity and potential for bias that this brings, is significantly reduced.

Whether or not you accept this, it is a useful argument to consider, because one of the striking things over the past decade in the United States, was the relative passivity of many people in the face of very intrusive government powers, a passivity that at least was partly driven by fear, understandably, but partly also driven by a pretty comfortable knowledge that it was unlikely to happen to people like me, that it was going to happen to other people. So saying that "this should apply to everyone" is a useful recasting of this.

Bias may still affect the manner in which data is organized and analysis prioritized, but it should be more evidence than the personal choices of individual analysts. It should leave a trail.

These three principles—the idea that intelligence should be public, it should be legal, and it should be consequence-sensitive—may sound obvious. They may even sound trite. Nonetheless, established democracies founded on the rule of law and the most important international organization on the planet have not lived up to them.

The United States only terminated a contract to outsource assassinations to Blackwater in June 2009, and we only know about it because Leon Panetta decided to go public. Britain has the most extensive CCTV regime in the world at the moment, and it is for the most part unregulated. The United Nations continues to maintain lists of

hundreds of individuals whose assets are frozen worldwide without requiring any evidence of wrongdoing, in some cases having held onto those assets for more than a decade, and even after the individual concerned has died.

The principles may also sound weak or pessimistic in addition to obvious and trite. The argument is not that this represents the best framework for intelligence; simply that it's the one most likely to have some traction both intellectually and politically.

Returning to the idea of a contract, embracing these principles should help to ensure that its terms at least are clear.

During debates on the Patriot Act in 2001, a U.S. Senator—I think it was Patrick Leahy—invoked the words of one of the Founding Fathers: "As Ben Franklin once noted, if we surrender our liberty in the name of security, we shall have nothing." But in fact Franklin's words were more nuanced. What he said was, "Those who would give up essential liberty to purchase a little temporary safety deserve neither liberty nor safety."

My contribution will not be the last word on how that relationship should be managed, but it is hoped that by reframing the question in the language of a social contract, maybe aided by a citizenry that are active participants rather than passive targets, it offers a framework to defend freedom without sacrificing liberty.

Thank you very much.

Questions and Answers

QUESTION: James Starkman. Thank you for a wonderful discussion.

Could you briefly comment on the WikiLeaks phenomenon as it impacts all these issues? Also, having served on the International Criminal Tribunal on Rwanda and—

SIMON CHESTERMAN: As an intern, I should emphasize.

QUESTIONER:—and your book, *Humanitarian Intervention and International Law*. How would you assess the probability that an intervention such as we have had in Libya would have saved hundreds of thousands of lives in Rwanda?

SIMON CHESTERMAN: I'll go backwards.

On Rwanda, I am not a military strategist, but Roméo Dallaire, who was the force commander on the ground at the time, argues quite persuasively, if he had had 5,000 troops—not air strikes, if he just had troops on the ground, because air strikes are pretty inefficient, as we are discovering in Libya, with this type of conflict—but especially in a place like Rwanda, where it was very densely populated and the weapons were machetes—if he had had 5,000 troops, he could have saved maybe 200,000 lives. It's absolutely true that if he had 5,000 troops he would have saved lots of lives. Exactly how many I don't know.

WikiLeaks is fascinating. I've been following this with great interest, not least because my brother spent some time on Magnetic Island, where Julian Assange grew up. We don't have any kind of connection to him. Two things I'll say about WikiLeaks. One is about secrecy and one about journalism.

First on secrecy, as I said at the beginning, this wonderful sociologist Edmund Shils wrote about the importance of denying secrecy to governments, and governments have been ever more secretive. WikiLeaks is interesting for the tidbits of information that we get, but most of it, apart from a couple of examples we've now heard—probably many people in the room know Carlos Pascual, the idea that he is the guy who has to resign because of a WikiLeaks thing—ending his term as ambassador early is tragic.

But most of what we found out is pretty uncontroversial. Berlusconi is vain—ah! Nicolas Sarkozy is thin-skinned—ah! Robert Mugabe is crazy—ah! I mean none of this is particularly interesting. [Laughter]

It's very telling, just on Libya, that we find out all these details about the Ukrainian nurse of Muammar Gaddafi—nothing about how he's going to get out of Libya, which would have been much more useful.

Julian Assange portrays himself as an advocate of transparency. There are two problems with that.

One is that we now know from the accounts of *The New York Times* and others dealing with Assange, the people who have come out of WikiLeaks—he is a notoriously private, secretive person in his own right; he's a little bit unstable in some ways. That's one problem.

The second problem is that the consequence of WikiLeaks is not going to be greater transparency or better decision making. It's going to be the exact opposite because the message that went around is: Be careful what you commit to writing, be careful what you tell people.

None of the apocalyptic versions are true. It's not going to stop countries sharing intelligence with the United States—that will continue. But it will make people much more careful what they put in writing and what they say in meetings, and all of that can lead to worse decision making.

It's worth nothing that the reason why it's alleged that Private Bradley Manning, who is now being severely mistreated—the reason why he had access to these hundreds of thousands of diplomatic cables is a result of September 11 and the need to share intelligence and information across the U.S. government. He had access to information that 3 million people had access to. One thing that has now happened is the State Department has taken these cables off SIPRNet, which is what he had had access to.

Secondly, much more briefly, on what this says about journalism. Throughout the modern history of intelligence, and in particularly in the late 20th and early 21st century, the two most important institutions in terms of accountability for intelligence agencies were firstly, the agencies themselves, self-restraint, the culture of the agency; secondly, the media.

Just in the last ten years, none of the big scandals in the U.S. context—warrantless electronic surveillance, extraordinary rendition, torture—none of them would have been public without quality investigative journalism.

WikiLeaks is quantity journalism and has no quality control, which means you can't tell what is relevant and what's not—which is why we have the kind of crazy Ukrainian nurse stories about Libya and not a close analysis of Libya. Also, it doesn't filter out the dangerous things, or at least not adequately. It's hard to prove any of this, but there are certainly comments from the Taliban that they had identified individuals and they were conducting their own investigations into people whose cooperation with the American forces in Afghanistan was going to be the subject of an al Qaeda, or at least a Taliban, investigation.

There are, first of all, reasons to be wary about being too enthusiastic about the triumph of WikiLeaks; and secondly, real reasons to be concerned about WikiLeaks, particularly when linked to the perilous financial situation of real investigative journalism.

QUESTION: David Mushner.

Do you look at the purpose for which information is gathered? Specifically, do you distinguish between information that is gathered in order to combat terrorism versus information that is gathered to result in criminal litigation?

SIMON CHESTERMAN: This has been a particular issue in the United States context in the last decade, with the Foreign Intelligence Surveillance Act, and there was litigation on this.

You're not referring to the Foreign Intelligence Surveillance Court and Court of Review cases, are you?

QUESTIONER: Yes

SIMON CHESTERMAN: You are.

FISA, the Foreign Intelligence Surveillance Act, adopted in the aftermath of Watergate, the Church and Pike hearings, in theory set a line that came to be, at least interpreted by many, as creating a wall between intelligence gathering for law enforcement and intelligence gathering for foreign intelligence purposes. This came to be widely misunderstood. It's now believed the Patriot Act was intended to tear down that wall. In fact, it reified a small portion of it.

At heart is for what purpose we collect information and intelligence. The highest court that considered this took a very narrow conception, that you only collect intelligence in order to do something, whereas in fact frequently intelligence is gathered just for the purpose of informing policymakers.

An example that I touch on in the book is if law enforcement observes an individual downloading child pornography, then there's an impetus for prosecution. This is a horrible crime.

If an intelligence official finds someone downloading child pornography, this is not something that you would necessarily want to prosecute. It's something that you might use to turn the person, either to persuade them to join your side, threaten them, get information out of them, or threaten to discredit them.

The purpose for which intelligence is gathered should ultimately be defined by the mandate of the organization.

This is something that I look at more directly in the context of Britain, where there have been more open debates about it.

Initially this was determined very broadly as "defense of the realm," and not really specified. In the British context, the mandate now includes guarding the economic interests of Britain, which is interesting in terms of industrial espionage.

Canada and Australia had long, agonized debates over this, and rejected terms like "guard against subversion," which has through history been used as a way of oppressing political dissenters, and ties the intelligence powers much more directly to preventing or identifying possibilities for politically motivated violence.

I'm partly responding, rather than answering your question, but there at two levels. One is the formulation of a mandate can be very important, and it must include things other than law enforcement.

Secondly, at the level of what you do with this, what you need is a much clearer line between law enforcement and other activities. In terms of organizational change in the United States, this is an argument basically to split the FBI into an intelligence-gathering capacity and a law enforcement capacity, because the main point at which the gathering of information has the potential for abusive powers or consequences on citizens is at the door of the courtroom, when the information actually becomes action.

QUESTION: Ernestine Bradley, the New School for Social Research.

My question has to do with disinformation. Maybe I'm totally naïve, but I assume that there is more disinformation circling the globe than we are aware of. Are there instruments that filter all information to find out what is "dis" and what is not? Or are we simply the victims of credulity, as it has happened with the weapons of mass destruction, which in retrospect was disinformation?

SIMON CHESTERMAN: Well, you can believe everything in the book certainly. [Laughter] I will answer in two parts.

First, there are two reasons why government intelligence services keep things secret. One is so that people don't know what you know. Another is so that people don't know what you don't know.

WikiLeaks to me was interesting for what was not there. There were some things that were not there. All of the WikiLeaks cables were at the secret level, so not top secret level, and that's why there's nothing about bin Laden. There was also virtually nothing on North Korea, and the assumption is not because all that is top secret, but just because we really don't know what is going on in North Korea.

Frequently you can do a great deal—and indeed, in *Legacy of Ashes*, a historian states that the CIA had a great reputation during the Cold War and a pretty terrible record. Despite the CIA itself being penetrated by, among others, Aldrich Ames—the people that the CIA turned in Russia were all walk-ins. Every Cuban agent run during the Cold War was a double agent, in fact working for the Cuban government. There are reasons to keep things secret like that.

How do you do quality control? You rely on gatekeepers of information. In the intelligence world you rely on your analysts, but in the public life you rely on good media.

Again, that is why I am, like so many, concerned about the rise of new media at the expense to some extent of old media, because much of the blogosphere is enormously interesting but inherently derivative, and it is commentary without investigative journalism. There are very few countries with organizations like *The New York Times* and *The Washington Post*, which can sustain that type of investigative reporting that is so important in at least getting closer to the truth.

JOANNE MYERS: Thank you so much, Simon. It is no longer a secret how intelligent and how wonderful your presentation was. Thank you very much.