Snowden and the future

Eben Moglen
Professor of Law and Legal History, Columbia Law School
moglen@columbia.edu

Part I: Westward the course of Empire

October 9, 2013

Good afternoon.

There is no introduction. After twenty-six years in this place it feels ridiculous to me to pretend that anyone is especially honored by my presence here.

If I am to be frank about it, I invited myself. Not in the way that Edward Snowden invited himself to Sheremetyevo Airport. Nor in the way that Julian Assange invited himself to the Ecuadorian embassy in London. Surely not in the way that Chelsea Manning invited herself to thirty-five years in Fort Leavenworth. No, law professor-like, I have assigned myself no onerous duties. I undertook nothing more than to come here and to tell you the truth.

I don't wish to press my ideas on anybody, but the truth is that I feel forced to speak myself. No one will remember much of what I have to say, but of the things about which I came here to speak — both those that have been done and those that remain to be done — I must say that they will never be forgotten.

In the third chapter of his *History of the decline and fall of the Roman Empire,* Edward Gibbon gives two reasons why the slavery into which the Romans tumbled under Augustus and his successors left them more wretched than any previous human slavery.

In the first place, Gibbon said, the Romans had carried with them into slavery the culture of a free people. Their language and their conceptions of themselves as human beings presupposed freedom. And thus, Gibbon says, oppressed as they were by the weight of their corruption and military violence, the Romans yet preserved for a long time the sentiments, or at least the ideas, of freeborn people. In the second place, the empire of the Romans filled all the world, and when that empire fell into the hands of a single person, the world was a safe and dreary prison for his enemies. It was, as Gibbon says, fatal to resist, and it was impossible to fly.

The power of that Roman Empire rested in its control of communications. The Mediterranean Sea, which was the transit hub of every western civilization, was their lake. Across their European empire, from Scotland to Syria, they pushed the roads — roads that fifteen centuries later were still primary arteries of European transportation.

Down those roads (which, as Gibbon says, rendered every corner of the Empire pervious to Roman power) the Emperor marched his armies. But up those roads he gathered his intelligence. Augustus invented the posts: first for signals intelligence, to move couriers and messages at the fastest possible speed; and then, for human intelligence, the carriages, so that, as Gibbon says, those who were present when dispatches were written could be questioned by the Emperor. Using that infrastructure and control of communications, with respect to everything that involved the administration of power, the emperor of the Romans made himself the best-informed human being in the history of the world.

That power eradicated human freedom. "Remember," says Cicero to Marcellus in exile, "wherever you are, you are equally within of the power of the conqueror."

The empire of the United States, the global empire that followed from victory in the Second World War, also depended upon control of communications. Possibly the greatest military lesson of the Second World War was that he who has access to his adversaries' military communications prevails. At every level, from the tactical artillery duel to the greatest strategic naval confrontations in the Pacific, the new pace of warfare gave victory to the one who knew the other side's plans first.

This was all the more obviously crucial in the development of the power to rule the world when, a mere twenty years later, the empire of the United States was locked in a confrontation of nuclear annihilation with the Soviet empire — a war of submarines hidden in the dark below the continents, capable of eradicating human civilization in less than an hour in an imperial confrontation whose rule of engagement was "launch on warning." Thus it was that the empire of the United States came to have precisely the same view of the rendering pervious to American power that had been the view of Emperor Augustus. And our listeners aspired to everything.

Now, the structure of listening which came out of the Second World War — the spying on signals, the stealing of signals, and the breaking of codes — this was, under everybody's understanding of the new order of power in the world, the crucial center of it all. And, while it has been commonplace to recognize since the end of the Cold War that the United States has spent for decades as much on its military might as all other powers in the world combined, it has not necessarily followed in people's consciousness that we applied to the stealing of signals and the breaking of codes a similar proportion of our diligence.

That system of listening, which had at its center the same reality of power, that system of listening grew up under the National Security Act and its successor legislation in the United States in a particular systematic form: listening under military command, controlling large civilian workforces. That structure, of course, presupposed precisely the foreign intelligence nature of the activity. Military control was both a symbol and a guarantee of the nature of the activity being pursued: Everybody understood that if you had put such activity domestically under military control you would have violated the fundamental principle of the civilian control of the government of the United States.

Instead what we had was a foreign intelligence service regarded as the most important basis of American power, responsible to the chief executive of the United States as commander-in-chief, and based in military control and military integrity. Because, of course, integrity was the other side of this coin. Military control ensured absolute command deference with respect to the fundamental principle which made it all "all

right," which was: "No Listening Here." The boundary between home and away was the boundary between absolutely permissible and absolutely impermissible — between the world in which those whose job it is to kill people and break things instead stole signals and broke codes, and the constitutional system of ordered liberty.

There's lots to be said — and we will need to say it as our time together goes by — about the morality of that assumption. But I must ask you to keep in mind that it also was accompanied by the reality of communications in the twentieth century, which were hierarchically organized and very often state-controlled. When the United States government chose to listen to other governments abroad — to their militaries, to their diplomatic communications, to their policy-makers where they could — they were listening in a world of defined targets. As to which they were roughly entitled to their favored assumption, which was that everybody else was listening back at them on those targets pretty much just as hard as they could, which was of course way less hard than we, because we were the Empire. On this basis, we formed fundamental alliances with the other English-speaking societies in the world for a complete cooperation of signals intelligence, based around two fundamental predicates: the listeners in each of the English-speaking societies were not listening at home, and they were not spying on one another. And therefore they and we stood back to back in their listening against the world. On that basis, in the era of the digital computer, we began to be capable of taking everything.

"Everything" was defined as all signals in the electromagnetic spectrum and its copper-wire accessories. The basic principle was: hack, tap, steal — where the roof of every U.S. embassy, and every American naval asset at sea, and every other place that we could cram antennas held the ones that we wanted to have there, and where every deal that we could make for exchange of signals intelligence among parties committed to listening gave us everything that we could get that we needed. Thus we could get what we needed, and we felt we needed it all.

In the beginning we listened to militaries and their governments. Later we monitored the flow of international trade as far as it indicated to us that it engaged American national security interests.

But there is this about the weapons of war: In 1937, bombing civilian populations from the air was an innovation in the criminality of war, and Pablo Picasso found it worthy of his work. Less than a decade later, dozens of the greatest cities in the world lay in rubble and the United States government had dropped nuclear weapons on cities in Japan. Now the United States government considers aerial bombardment to be the cleanest form of war.

In the beginning, we listened to armies, embassies, diplomats, government officials. Then we listened to the global economy. Now we are being told that spying on entire societies is normal.

The regime that we built to defend ourselves against nuclear annihilation, in a world where access to the other fellow's signals is what makes victory, came at the end of the twentieth century under two forms of profound social restructuring. In the first place, the Cold War ended and the Soviet Union dissolved. An entire establishment of national security — which continues to absorb more resources in the United States than in all the rest of the world put together, and I am including the listeners — an entire

national security structure re-purposed itself, not to spy upon an empire with twenty-five thousand nuclear weapons pointed down our throats, but at the entire population of the world in order to locate a few thousand people minded to various kinds of mass murder.

In the second place, the nature of human communication changed. The system that they built, with all of its arrangements, was dependent, as I said, upon fixed targets: a circuit, a phone number, a license plate, a locale. The question of capacity was about how many targets you could simultaneously follow in a world where each of them required hack, tap, steal. But what happened at the beginning of the twenty-first century was that we acquired a new way of communicating in the human race — the beginning of the beginning of the beginning of the nervous system we are building in which each human being is a neuron in that great hive-mind called humanity. And from the moment we began to do that, two things began to fail: the simplicity of "one target, one circuit" went away, and the difference between inside and outside vanished too.

In particular, it vanished in the United States, because so much of the intelligence of the brain being built for humanity, for better and for worse, resided here. Therefore, the question "Do we listen inside?" came to seem like a question about "Are we going to lose the ability to listen at all?" About which, of course, fundamental doctrine of national security — whatever "national security" means — had only one acceptable answer.

Into this mixture of the structures of the twentieth-century imperial power and the realities of twenty-first century technology, a vastly imprudent American administration then intervened.

Whatever else history will record of them, it will record of them that they didn't think long before acting. Presented with a national calamity which also constituted a political opportunity, nothing stood between them and all the mistakes that haste can make for history to repent at leisure. And what they did, of course — in secret, and with the assistance of judges chosen by a single man operating in secrecy, and with the connivance of many decent people who believed themselves to be doing the only thing that would save the State — was to unchain the listeners from law.

Not only had circumstances destroyed the simplicity of "no listening inside," not only had fudging with the Foreign Intelligence Surveillance Act carried them into the land where law no longer provided them with useful landmarks, but they wanted to do it — let's be frank: they wanted to do it. Their view of the nature of human power was Augustan, if not august, and they wanted what it is forbidden to wise people to take unto themselves. And so they fell, and we fell with them.

Our journalists failed. The *New York Times* allowed the 2004 election not to be informed by things that it knew, having made a decision which, no matter how many Pulitzer prizes it goes on to win, will always be a pain in our recollections (if not elsewhere).

We failed collectively to show any outrage, because we were afraid. We did not demand the end at the beginning. And now we're a long way in. We had our Guernica and we paid little attention. And there weren't any limits any more. They were living in an evolving net, with conscriptable brains gathering intelligence on all the human

race for mere purposes of bagatelle and capitalism. So they perverted those places. And to the network operators we gave legal immunity in the United States for complicity, thus easing the way further.

And then there began a revolt inside.

In Hong Kong, during his brief career as a public thinker and speaker — which I commend to your attention and which we will spend much time talking about in future times together — in his career as a public commentator, Edward Snowden said a very straightforward and useful thing. He said: analysts are not bad people, and they don't want to think of themselves that way, but they came to calculate that if a program produced anything useful, then it was justified.

Because, of course, it was not their job to weigh the fundamental morality. Which is too bad, because the people whose job it was to weigh the fundamental morality failed more bitterly than we, and our journalists, and our everybody.

They fell, and we fell with them, because they refused to accept that there is a morality of freedom. And it was the people who worked for them who felt their failure first. So, from the middle of the first decade of the twenty-first century, people began to blow whistles all over the field.

Those courageous people sacrificed their careers, frightened themselves, sometimes suffered personal destruction, to say that there was something deeply wrong. Later I shall try and show you both how they came to those conclusions and what they tried to say. But it is sufficient for the moment to say that what happened back was Rule By Fear. It will be sufficient to say that, in their unwisdom, those who believed in the importance of the listeners and their activities sought to deal with those who blew the whistle by the harshest possible treatment.

It is unfortunate to have to dwell on the extent of the failures, once the morality of freedom was no longer part of their world. Mr. Snowden said in Hong Kong that he was sacrificing himself — which he knew he was doing — in order to save the world from a system like this one constrained only by policy documents. Next time we meet we shall think long and hard about the political ideas of Edward Snowden — they are worthy of your respect and your deep consideration. But for now, once again, it will be sufficient to say that he was not exaggerating the nature of the difficulty.

Because of Mr. Snowden, we now know that the listeners, in their aggressive effort to maintain the security of the United States by breaking anything that stands in the way of listening, undertook to do what they repeatedly promised respectable opinion in the trade they would never do.

Systematically, they attempted what they had once and for all promised many a time in the discreetest but most credible fashion to respectable opinion, which then carried their water for them throughout our world. They always said they would not attempt to break the crypto which secures the global financial system.

That was false.

When, on September 6th, the New York Times re-entered the pursuit of journalism in this area so triumphantly, by revealing the existence of BULLRUN, publishing Mr. Snowden's various disclosures concerning both the substance of BULLRUN and the National Security Agency's discussions of it, we learned that the United States

listeners had been systematically and deliberately trying to subvert the crypto that holds the international financial system together, for years. And we learned a good deal more — which we shall spend more time upon on another evening, considering carefully what we learned in this respect — we learned that their efforts had been so far only partially successful.

Within hours, they had forfeited respectable opinion around the world, which had stood solidly in their corner all the way along. The recklessness of what they had done, and the danger to which it put the people in the world who don't accept danger from the United States government, was breathtaking.

When the morality of freedom is so thoroughly thrown away, it isn't *only* the "little people" of the world who suffer, but they do.

The empire of the United States, the one that secured itself by listening to everything, was the empire of exported liberty. What we had to offer all around the world was freedom — after colonization, after European theft, after the forms of twentieth-century horror we haven't even talked about yet — we offered liberty; we offered freedom.

In the twentieth century, we were prepared to sacrifice many of the world's great cities, and to accept the sacrifice of tens of millions of human lives, in order to secure ourselves against forms of government we called "totalitarianism," in which a State grew so powerful and so invasive that it recognized no longer any border of private life, and brought itself into everything that its subjects did, so that the State listened to every telephone conversation, and kept a list of everybody every troublemaker knew.

So let us tell the unfortunate truth as it appeared to the people who worked within the system: When the morality of freedom was withdrawn, our State began fastening the procedures of totalitarianism on the substance of democratic society.

There is no historical precedent for the proposition that the procedures of totalitarianism are compatible with the system of enlightened, individual, democratic self-government. No one has ever previously in the history of the human race evolved an argument — and, as I will show next time, no argument can be evolved — that would give us any confidence in the ability of the procedures of totalitarianism to coexist with those of constitutional democratic self-government. It is enough to say for now that omnipresent invasive listening creates fear. And I need not be Justice Brandeis to tell you that fear is the enemy of reasoned, ordered liberty.

It is, of course, utterly inconsistent with the American ideal to attempt to fasten the procedures of totalitarianism on American constitutional self-government. And this summer many of my dear colleagues and comrades in our movement have spent a lot of time in the United States pointing out that all of this is deeply inconsistent with some important American right not to be listened to. Which right I too have, with them, and believe in deeply, but which it is not my point, primarily, to assert just this moment. Partly, as I shall suggest next time, because freedom is merely privilege extended unless enjoyed by one and all. But primarily because there is an even deeper inconsistency between American ideals and the subjection of every other society on earth to the procedures of totalitarianism.

Freedom hath been hunted round the globe. Asia and Africa have long expelled her. Europe has been bullied into treating her like a stranger and England would take her into detention at Heathrow should she arrive. The President of the United States

has ordered everyone not to receive the fugitive, and to prepare in time an asylum for humankind.

You see how it works when you rewrite Tom Paine without the morality of freedom. And so our primary problem right now is that we allowed them to export slavery to the world. All of which, in one form or another, became clear, in one mind after another, within the bowels of the empire and its listeners over the last decade.

William Binney — with whom we shall spend some time along the way — said in a public speech, "I left the NSA because the systems that I built were turned against you. We had a legitimate charter in foreign intelligence gathering, but then they went and turned those systems against you — I didn't mean it, but they did it. And so I left."

People began to understand, within the system, that it was being sustained against democratic order, not with it. Because they knew that what had come unmoored had come unmoored in the dark and was sailing without a flag. They were good people, and they began to break. And when they broke, the system broke them back. In the end, at least so far — until tomorrow — there was Mr. Snowden, who saw everything that happened and watched what happened to the others.

He understood, as Chelsea Manning always understood, that when you wear the uniform you consent to the power. He knew his business very well. Young as he was, as he said in Hong Kong, "I've been a spy all my life," and I believe him. And so he did what you have to have great courage to do, wherever you are, in the presence of what you believe to be radical injustice. He wasn't first, he won't be last, but he sacrificed his life to tell us things we needed to know.

Edward Snowden committed espionage on behalf of the human race. Knowing the price, knowing the reason, knowing that it wouldn't be up to him whether sacrificing his life was worth it.

So I would think that our most important effort, first, is to understand the message: to understand its context, to understand its purpose, to know its meaning, and to experience the consequences of having received the communication.

Others will of course regard the first imperative as to eliminate the message, and the messenger, and the meaning: to render everything as invisible as possible. Because invisibility is where listeners have to live in order to work. But I think we must let them go about that business. We must let them try to obliterate the message as best they can, and do our work, which is the work of understanding first.

It will be difficult to judge, when you come to the moment where you consider yourself either entitled or obliged to begin doing so. The reason that it will be difficult to judge is that there is always much to say on both sides when someone is greatly right too soon.

In the United States, those who were "premature anti-fascists" suffered later. It was right to be right when all others were right. And it was wrong to be right when only the people we didn't want to be were already there.

I need not explain to you that it is possible to consider a man a terrorist who tried to do too soon what we took four years and 750,000 lives in order to achieve, namely to free the slaves. And I do not need to explain to you why it is that Gibbon considered

the master key to the tender respect of Augustus for a free constitution, which he had destroyed, to be his fear.

The death of Caesar was always before his eyes, says Gibbon, and this shaped his principles in politics. Augustus was sensible, says Gibbon, that mankind is ruled by names; and he was not deceived in his expectation that the Senate and the Romans would submit to slavery, so long as they were respectfully assured that they kept all their ancient freedom.

So there are some pieces that we need to put together in order to understand. In the first place, we must see the politics of now, both as Mr. Snowden saw it, thus bringing us the message we must live with, and as we see it in ourselves.

We shall consider, next time, the politics of our condition, and I shall suggest to you that it lies in this: If we are not doing anything wrong, we have a right to resist. The nature of our freedom is that we lose it because we do not exercise it. And the nature of our freedom is not necessarily the one we find only in the books of law.

We shall consider two constitutional traditions in the United States next time: one made by European people running away to be free, and one made by African people, forced into slavery, who had to run away, in the United States, in order to be free. Two constitutional traditions of resistance — differently structured and equally in our bones.

And we must consider the relation that we have to the rest of the human race in this, and ask ourselves whether we are seeking privilege or something that belongs to all of humankind. For which it will be necessary to understand the ideas of those who have risked their lives to inform us, not because their ideas are necessarily privileged above our own, but because they have sad experience from which to speak, and we should hear them.

We must think about the role of all those working people in the systems, both private and public, which constitute spying on humanity. We must ask what they are telling us in their resistance and what our side in their resistance ought to be. That workers were complaining in the Gulf last week was making a question for global football. We might want to be at least equally concerned with what we have learned from the workers inside the matrix all this while.

We must ask what it means — both in the private and in the public world of listening and spying and analyzing and concluding, and how we might consider this thing that we're now calling "privacy," in relation to the thing that we used to call freedom.

But of course, in the end, all of this would not be worth talking about here, much less your coming to listen to me talk here, unless we were going to talk about what we are actually going to do. If the problem is that we slept too long, then plainly Mr. Snowden did not come but to wake us up.

We shall see that there are both legal and political forms of resistance around the world that we must all engage in. And I shall show next time, as best I can, the possibilities down which we may choose to take ourselves in that regard. But we must also change the way we communicate, so as to restore the balance between what they can and what they can't do.

Here lies the secret of Mr. Snowden's enormous sacrifice and their enormous anger. Because the center of what Mr. Snowden has done is to tell us what armor still works. He has spent his life now for us, to tell us what we still have time to do if we want to restore to the technology of our communications the morality of freedom.

He has been quite precise. He has been quite careful. He has been most thorough. He understands his business. He has spied on injustice for us and he has told us what we need to know. Despite the efforts, continuing every instant, all around us, in a world becoming a safe and dreary prison for their enemies, he has told us what we require in order to do the job and get it right. And if we have a responsibility at all, then part of our responsibility is to learn, now, before somebody concludes that learning should be prohibited.

Which never happens in a free society.

I wish we weren't here. I don't wish that I wasn't here more than I wish you weren't here. I wish us all out of this war. Twelve years — the longest war in history of this society, nowhere concluded, nowhere near finishing, nowhere capable of being defined as done.

We went from listening to armies and embassies to listening to global trade and now we are fastening spying on entire societies, with a skill and energy that only a growing empire can still manage. We shall talk about the world where a nation of 1.3 billion people gains a Content Monitoring System in sixteen months, against the ordinary suppositions of every Indian person who thinks, "They can't do that." But, thanks to the new Bechtel, Booz Allen Hamilton — erstwhile employer of one Edward J. Snowden — yes they can.

The procedures — mind you, only the procedures — of totalitarianism are a leading American export these days. I wish we weren't here. I wish that everything we thought we did in the twentieth century we had accomplished. I wish we had defeated totalitarianism. I wish we had eliminated smallpox. I wish that we were growing the Net that we deserve to have, in which every human brain could learn and every human being could grow, nourished by the knowledge and the support of all the others.

There may come a day ... but if we have only one more river to cross before we get to freedom, it's a deep one, and it runs fast the other way. And those who want to bring us out are going to be called traitors — they are. And God forbid that they should lift their hands in anger, or they will be slaughtered. And those who do it will feel they have all right on their side.

It is wrong to be right too soon.

It's wrong to be right too soon, but it is not too soon to be right now. Because if we're not right now, then they will remember our failure for fifteen centuries. And they will say of us, oppressed by the weight of our corruption, and our fear of terrorist violence, that we were ready to submit so long as we were assured that we possessed our ancient freedoms. And as for everybody else — if not "Civis romanus sum," then who are you?

Which is no way for us to be talking. Not now, not ever.

We have wandered so far into the dark that we have lost who we are. Like many a tragic figure in history, Mr. Snowden went further out into the dark in the hope that he could lead us back.

We had better do our best to learn from him what we can, as we watch his light vanish into the darkness.

Part II: Oh, freedom
October 30, 2013

Since we were last here the press of the world has been full of information concerning the practices of the U.S. listeners, and statements from presidents, premiers, chancellors, and senators on the subject.

Our purpose this time being to consider the political meaning of Mr. Snowden and the future he has brought us, we must begin by discarding for immediate purposes pretty much everything said by the presidents, the premiers, the chancellors, and the senators. It has been a remarkable display of misdirection, and misleading, and outright lying. We'll come back to it, but it will not serve us at the outset.

It is indeed really what doesn't matter — all the froth that we've been reading since we were last together, from the respondents. We need to keep our eye on the thinking behind Mr. Snowden's activities — which he has done much more to explain since we were last together — and we need to understand the message he has sent us. And so, for that purpose, I come again before you.

What matters most — and what it has been the goal of the presidents, the chancellors, the premiers, and the senators not to say — is how deeply the whole of the human race has been ensnared in the process of pervasive surveillance that destroys freedom.

The fastening of the procedures of totalitarianism on the human race is the political subject about which Mr. Snowden has summoned us to an urgent inquiry. And it is that inquiry which it has been the goal of pretty much everybody responding on behalf of any government or state not just to ignore but to obscure.

We begin therefore where they are determined not to end, with the question whether any form of democratic self-government, anywhere, is consistent with the kind of massive, pervasive, surveillance into which the United States government has led not only us but the world.

This should not actually be a complicated inquiry.

For almost everyone who lived through the twentieth century — at least its middle half — the idea that freedom was consistent with the procedures of totalitarianism was self-evidently false.

Those who fought against it, those who sacrificed their lives to it and had to begin again as displaced persons and refugees around the world, and those who suffered under the harrow of it were perfectly clear that a society that listens to every telephone call, and spies on every meeting, and keeps track of everybody's movements is incompatible with a scheme of ordered liberty, as Justice Benjamin Cardozo defined American constitutional freedom.

But at the beginning of the twenty-first century, what seemed clear and absolutely unnecessary to inquire into in the twentieth is now, apparently, a question.

So we had better address it directly.

A large number of people in the United States have in their family tree, in their genetic material, in their understanding of the world, awareness of a system that made everybody keep track of their movements and have a pass, that gave some people the right to scrutinize every communication of everybody else, that made every home

subject to intrusion and disruption at the whim of other power. For those who have tasted the bitterness of slavery in their past, it should not be necessary to explain why the rules — however velvet the glove in which they are contained may be, however invisible the system within with they are embedded — the system that keeps track, the system that listens everywhere, the system that knows no boundaries, in America, is slavery.

We should not need to inquire, carrying as we do our own history closest, whether a system of power which listens everywhere, which can go everywhere, which keeps track of everybody's thoughts and feelings and speech, is inconsistent with freedom. We know, because we have lived on both sides of such a system. And we know its evil.

But let us forget what we have learned by bitter experience, what we carry in our own chests, let us forget it, let us put it aside, let us be law professors, shall we, and political scientists:

For analytical purposes, let us take this word "privacy" that we are using quite freely, and take a little bit more care about what it really is.

Privacy — as we use the word in our conversations now, all around the world, and particularly when we talk about the Net — privacy really means three things:

Secrecy: our ability to keep messages "private," so that their content is known only to those who we intend to receive them.

Anonymity: our ability to keep our messages — even when they are open — obscure as to who has published them and who is receiving them. Anonymity is about both publishing and reading.

Autonomy: our ability to make our life decisions independent upon force which has violated our secrecy or our anonymity.

These are the principal components of the thing that we call "privacy." You will discover, as you look at it more closely, that with respect to each, we are talking about a precondition to the order that we call "democracy," "ordered liberty," "self-government," to the scheme that we call in the United States "constitutional freedom."

Without secrecy, democratic self-government is impossible, because people may not discuss public affairs with those they choose, excluding those with whom they do not wish to converse. If you have lived in a society where in every dorm room, every work place, every public transport vehicle, there was an agent, whose job it was to listen and inform, and if you think about the consequences for political conversation in that neighborhood, you need go no further. If you are fortunate enough never to have had that experience, most of your comrades around the world can enlighten you.

Anonymity is necessary for the conduct of democratic politics. The United States Supreme Court took until 1995 to recognize it, but it recognized it, and to Justice Stevens we owe a clear statement of the importance of anonymous political conversation at the core of the First Amendment. The cases in which the Court has considered anonymity and its rights are precisely cases about political communication, central cases about the exercise of democracy — cases about accountability for taking political opinions that one wishes to keep one's name off. It is, as Justice Stevens noted in that inquiry, not terribly surprising that our greatest artifact of divine wisdom with

respect to our constitution — a set of political pamphlets penned by three very slippery characters called Hamilton, Madison, and Jay that we refer to as *The Federalist Papers* — was of course published under a pseudonym.

That autonomy is altered by the invasion of secrecy and privacy, that free decision-making is impossible in a society where every move is monitored, those of you who have friends in North Korea may enquire into directly, if you please. But any conversation with those who lived through twentieth-century totalitarianisms or any contact with the realities of American slavery will surely clear it up for you.

In other words — though it shouldn't be necessary to demonstrate, though we ought to have taken the bitter experience of American history in the nineteenth century and the history of the West in the twentieth for sufficient demonstration — for those who really do like ignoring the facts and working it out with chalk, privacy is a requirement of democratic self-government. The effort to fasten the procedures of pervasive surveillance on human society is the antithesis of liberty.

This is the conversation that all the "Don't listen to my mobile phone!" has been not about for the last two weeks. If it were up to power, the conversation would remain at that phony level forever.

So we are, at the moment — thanks to Mr. Snowden, who has precipitated what even his adversaries now like to call a "necessary conversation" — we are now in a necessary conversation in which on the other side there parties who do not wish to explain exactly what they do, and advanced, and will advance, no convincing argument that what they do is compatible with the morality of freedom, with American constitutional law, or with the human rights of every person in the world. They will not offer an argument. They will certainly not offer a defense. They will instead attempt, as much as possible, to change the subject, and, wherever they cannot change the subject, to blame the messenger.

But what you have seen around the world in the last two weeks is the evidence that this is extremely unlikely to work.

And so we need to consider the political environment created by what has happened, before we can begin to address the more or less empty rhetoric that has been assigned to the presidents, the chancellors, and the premiers.

"Why are they operating in this way," you may ask nonetheless, "as though everybody were on the same side?"

Here the history is very clear and remarkably available. One does not need access to classified documents to see — in records we will be making public as part of our effort in "Snowden and the future" over the next two weeks — it is very easy to see how the military and strategic thinkers in the United States adapted to the end of the Cold War by planning pervasive surveillance of the world's societies.

In the early nineties, in documents that are in no way secret, the strategic and military planners made clear in the United States in a range of fora — the think tanks, and the Pentagon, and advanced research reports, and in a variety of other ways — that they foresaw, as indeed we now observe, a world in which the United States had no significant state adversary, and found itself locked in a series of "asymmetric conflicts." That was the phrase, meaning "guerrilla wars."

In the course of that thinking, in the redefinition of the U.S. posture and threat assessments and strategic posture after the end of the Cold War, the American military strategists and their intelligence-community colleagues came to regard American rights in communications privacy as the equivalent of sanctuary for guerrillas.

The documents are very clear in describing precisely that relationship, circa 1992–1993, in which it was understood that in future asymmetric conflicts the adversaries — that means people, you understand, bad people committed to bad activity but small groups of individuals affiliated with and possessing the power of no state — these people would use communications facilities which benefited from American civil liberties as sanctuary, and that it would be necessary to go after the "sanctuaries."

Of course, this was the position of military strategists and their listener colleagues. It was not national policy, but it was an important part of the policy formation discussion, albeit relatively quiet. There were, of course, political adults in the room. And while the United States government considered various efforts at improving its ability to listen to encrypted communications in the mid-nineties — the Clinton administration had the Clipper Chip initiative, for example — and there were also significant efforts to ensure that domestic law enforcement would not be disadvantaged by the movement to digital communications, which led in 1995 to the CALEA statute concerning the availability of "wiretapping" technical facilities in digital telephone systems that didn't natively offer them — a compromise which split the nascent Electronic Frontier Foundation into two camps, one of which became CDT — although there were steps taken to facilitate not only the work of the domestic law enforcement agencies but also the listeners within the United States — as we now know, as we see the evolution of the FISA statute in the FISA court, in secret judicature we couldn't see before — still and all there was a clear understanding that this idea of denying "sanctuary" by breaching American civil liberties in U.S.-based communications was not part of the senior policy-making dialogue. It was part of what one team constantly pushed for, as they did after the first World Trade Center bombing, after the Africa embassy bombings, after the *Cole*. The whole pervasive surveillance system, not just the Patriot Act but all the pieces that we now understand surrounded it in the secret world's understanding, were constantly advocated for at the end of the twentieth century, and as constantly rebuffed.

And then, as we saw last time, at the opening of the twenty-first century, an American administration which will go down in history famous for its tendency to think last and shoot first bought — hook, line, and sinker — the entire scheme, and, within a very short time after January 2002, mostly in secret, put it all together.

The consequences around the world were remarkably uncontroversial. By and large, states approved or accepted. Some of this happened because the United States government was even then using quite extraordinary muscle around the world — after September of 2001, you were with us or against us. But it also happened because so many other governments had come to base their national security systems in part on cooperation with American listening. And after the declaration of the new Global War on Terror, that was made more true.

By the time the present administration had settled into office in the United States, as one senior official with relevant responsibility described it to me halfway through the first term of the current administration, in our government-to-government relationships

about the Net, "all of us — the Chinese, the Europeans, and us," that was "all of us" at the table, "— we all agree about one thing," this senior official of the U.S. government said to me before the start of this decade: "We all agree about one thing: about exfiltration." (This is the listeners' word for spying: "exfiltration." They "exfiltrate" data off our networks into their warehouses.) "We all agree," this official said, "about exfiltration: Everybody agrees that it can't be stopped and it shouldn't be limited. We disagree about what kinds of intervention," that is, breaking things in the Net, "should be allowed."

The important point in this one conversation (on which I hinge nothing — you can find this statement again and again, in unclassified documents, from this administration, even) — the important point was that American senior policy makers thought there was general consensus around the world that everybody could listen to everybody's societies: It could not be stopped; it shouldn't be limited. The Chinese agreed. The Americans agreed. The Europeans agreed, which really meant of course that they were dependent on American listening and hadn't a lot of power to object.

Nobody told the people of the world.

What was common understanding among the policy-making elite — who governed among them still only about a third of the world's population — the policy-making elite was pretty much convinced that global civil society was a free-fire zone for everybody's listeners, and there wasn't anything to be said about it — particularly not to all those people, who were supposed to not know.

This is the condition upon which the whistles started to blow all over the field, as I said last time. Throughout the situational ethics of all of this, a few people — all of them in the English-speaking world, all of them people who came from societies with strong traditions of the rule of law, protection for whistle-blowers, some form of civilian political control over domestic security intelligence — whistle-blowers began to speak up.

Mr. Snowden saw what happened to precedent whistle-blowers, and behaved accordingly.

What had opened by the end of the first decade of the twenty-first century was a gap between what the people of the world thought their rights were and what their governments had given away in return for intelligence useful only to the government — a gap so wide, so fundamental to the meaning of democracy, that those who operated the system began to disbelieve in its legitimacy. As they should have done.

Mr. Snowden's political theory has been quite exact and quite consistent. From his first statements in Hong Kong, through his interview with James Risen of the *New York Times*, to his statement over the weekend, sent to our colleagues and comrades in Washington, D.C., seeking to have them stop watching us (whoever "us" might be), Mr. Snowden has been very clear: The existence of these programs, undisclosed to the American people, is a fundamental violation of American democratic values. Surely there can be no argument with that.

Mr. Snowden's position is that efforts so comprehensive, so overwhelmingly powerful, and so conducive to abuse, should not be undertaken, save with democratic consent. And Mr. Snowden has expressed recurrently his belief that the American people are entitled to give that consent.

But Mr. Snowden has also identified the fastening of those programs on the global population as a subject which deserves a form of moral and ethical analysis that goes behind mere *raison d'état.*

Mr. Snowden said again to Mr. Risen, in some detail, what he had suggested in his statements in Hong Kong: We have dealt with terrorists and rogue states before. We do not need to do all of this in order to achieve control over those problems. People have acted, Mr. Snowden said, as you will recall — analysts are not bad people, and they don't want to think of themselves as bad people — but they have adopted a misleading metric: They think if a program produces anything it is justified.

Because of course the very essence of democracy is that it is for the people to judge what is justified with respect to the entrenchments of their rights and invasions thereto.

I think that Mr. Snowden means — as certainly I and my comrades mean — that in the exercise of the democratic discretion to determine whether we wish to fasten these procedures of totalitarianism on other people in the world, that we should consider our values as extending beyond our borders, and that we should make those decisions not in the narrow, selfish self-interest that is *raison d'état,* but with some sense of what it is appropriate for a beacon of liberty to humanity to do.

We will speak, of course, about American constitutional law and about the importance of American legal phenomena — rules, protections, rights, duties — with respect to all of this. But we should be clear in our minds that, when we talk about the American constitutional tradition with respect to the avoidance of slavery, we're talking about more than what is written in the law books.

We face a system in which the States have, almost without exception, agreed complicitously to deliver over their people to a form of pervasive spying which we know is incompatible with our own liberty and with the liberty that we have frequently postured in the world as bringing to the human race as a whole. We know this. As individual citizens, we are now aware. Mr. Snowden has made it impossible for us to ignore this fact unless we bury our heads so deep in the sand that we are likely to suffocate.

But we face two claims — you meet them everywhere you turn — which are basically the politics against which we are working. One argument says, "It's hopeless, privacy is gone, why struggle?" The other one says, "I'm not doing anything wrong, why should I care?"

And these — neither one of them a brilliant argument from a political point of view — these are actually the most significant forms of opposition that we face in thinking about what we need to do in the political situation in which we find ourselves.

The premise of my being here before you is that it is far from hopeless. Mr. Snowden has described to us, as I told you last time, what armor still works. Mr. Snowden's purpose was to explain to us how to distinguish between those things hopelessly corrupted and no longer usable, those things endangered by a continuing assault on the part of an agency gone rogue, and those things which even with their vast power, all their wealth, and all their misplaced ambition, conscientious, and effort, they still cannot break.

Hopelessness is merely what you are supposed to get, not what you have.

And so far as the other argument is concerned, we owe it to ourselves to be quite clear in response. My own personal position I recommend to my comrades around the world: If we are not doing anything wrong, then we have a right to resist.

If we are not doing anything wrong, then we have a right to do everything we can to maintain the traditional balance between us and power that is listening. We have a right to be obscure. We have a right to mumble. We have a right to speak languages they do not get. We have a right to meet when and where and how we please so as to evade the paddy rollers.

We have an American constitutional tradition against general warrants. It was formed in the eighteenth century for good reason. It puts the limit of the State's ability to search and seize at what you can convince a neutral magistrate, in a particular situation — about a place, a time, a thing — is a reasonable use of governmental power.

That principle was dear to the First Congress, which put it in the Bill of Rights, because it was dear to British North Americans, because in the course of the eighteenth century they learned what executive government could do with general warrants to search everything, everywhere, for anything they didn't like, and use local police to do it. That was a problem in Massachusetts in 1761, and it remained a problem until the end of British rule in North America. And still it was a problem, because the presidents, premiers, chancellors, and senators back then were also unprincipled in their behavior. (Thomas Jefferson talks a better game than he plays, but never mind.)

The principle is clear enough; but there are only nine votes in the United States that count on that subject right now, and we must wait to see how many of them are prepared to face the simple unconstitutionality of something too big to fail — a challenge for a Justice, a thing that makes a lifetime in the history books one way or the other. Those nine votes are the only votes that matter about that, and we must go about our business in other ways.

The First Amendment, too, as I have pointed out, conveys to every listener in the twentieth century a message in favor of privacy and anonymity and the ability to speak freely to whom one chooses, without being forced by government to disclose. I remember *NAACP vs. Alabama.* But the NSA was never really schooled in the idea that the social graph of the United States is nobody's damn business.

When a senior government official said to me in March of 2012, "Well, we know we need a robust social graph of the United States," I said, "Let's talk about the constitutionality of that for just a moment. You mean you're going to take us from being a free society to a society in which the federal government keeps a list of everybody every American knows. You're proposing to do that with, say, a law?" And he just laughed. Because they did it with a document signed by the Attorney General and the Director of National Intelligence, released after dark on a rainy Wednesday night in March. No legislation at all was necessary, or at any rate they thought it wasn't. That was when they decided to take all the information about Americans about whom nothing is suspected and, instead of ditching it after eighteen months, to keep it for five years, which is the equivalent of forever. That was an administrative decision — no law at all.

So what we found ourselves living with we could think of as unconstitutional, in that sense. But I would urge you to consider the possibility that there exists a second

American constitutional tradition, also relevant. You see, the American constitutional tradition we admire in the books was made by people, mostly, who fled Europe and came to North America in order to be free, and it is their activity, politically and intellectually, which we find deposited in the documents that made the Republic. But there is a second constitutional tradition, and it was made by people who were brought here without their will being involved, and had to run away here in order to be free. And that constitutional tradition is slightly different in its nature, though it conduces, eventually, to a similar result.

Running away from slavery is a group activity. Running away from slavery requires the assistance of those who believe that slavery is wrong. The people of the United States have forgotten how much of our constitutional tradition was made in the contact between people who needed to run away in order to be free and people who knew that they needed to be helped because slavery was wrong.

People in the United States have now forgotten that, in the summer of 1854, when Anthony Burns, who had run away from slavery in Richmond, Virginia, was returned by the federal court in Boston, Boston itself had to be placed under martial law for three whole days. Federal troops lined the streets as Anthony Burns was marched down to Boston Harbor and put aboard a ship to be sent back to slavery. If Boston had not been held down by force, it would have risen.

When Frederick Douglass ran away from slavery in 1838, he had the help of his beloved Anna Murray, who sent him part of her savings to travel on, and who sent him the sailor's clothing that he wore. He had the help of a free black seaman who gave him those identity papers. He had the help of many dedicated people who risked many things — property and life — to help him reach New York.

We fought slavery, as Frederick Douglass pointed out, long before Abraham Lincoln wanted to — though he may have hated it, as Douglass mentioned in the great memorial in 1876 for him, he may have hated it with his whole soul.

Our constitutional tradition is not merely contained in the negative rights to be so famously found in the Bill of Rights. It is also contained in the proposition that liberty must be given to everybody, always. That it must be accorded people as a right. That slavery is wrong. That it cannot be tolerated. That it must be fought, and that the way to fight it is to help people be free.

And so the constitutional tradition we should be defending, now, as Americans, is a tradition which extends far beyond whatever boundary the Fourth Amendment has in space, place, or time. We should be defending not merely a right to be free from the oppressive attentions of the national government, not merely fighting for something embodied in the due-process clause of the Fourteenth Amendment after 1962, because of a trunk of smut left behind by a departing lodger in Mrs. Mapp's boarding house in Ohio. We should be rather be fighting against the procedures of totalitarianism because slavery is wrong; because fastening it on the human race is wrong; because providing the energy, the money, the technology, the system for subduing everybody's privacy around the world — for destroying sanctuary in American freedom of speech — is wrong.

And if we're going to exercise our democratic rights in the United States as Mr. Snowden wishes us to do — and has given us the most valuable thing that democratic self-governing people can have, namely information about what is going on — if

we are to do all that, then we should have clear in our mind the political ideas upon which we ought to be acting. They are not parochial, or national, or found in the *U.S. Reports* alone.

A nation conceived in liberty, and dedicated to the proposition that all men are created equal, enslaved millions of people. It washed away that sin in a terrible war. We should learn from that, as we are called upon now to do.

The politics that we have as Americans are slightly more complicated, but they are fundamentally the same as the lines upon which our colleagues and comrades around the world must also move. Everywhere citizens must demand two things of their governments:

In the first place, you have a responsibility, a duty, to protect our rights by guarding us against the spying of outsiders. Every government has that responsibility. Every government has the responsibility to protect the rights of its citizens to be free from the intrusive spying of outsiders. No government can pretend to sovereignty and responsibility with respect to its citizens unless it makes every effort within its power and its means to ensure that outcome.

In the second place, every government around the world must subject its domestic listening to the rule of law.

Now this is the tragedy, where the overwhelming arrogance of the listeners has left the American government. The government of the United States could have held up its head until the day before yesterday and said that its listeners, unlike all the other listeners in the world, were subject to the rule of law. It would have been an accurate boast.

To be sure, the rule of law even in the last generation was somewhat corrupted by secret judicature, and courts appointed by a single decision maker, and so on, and so on. But the truth is that American listening was subject to the rule of law as no one else's was in the world or is now.

For nothing, history will record, they threw that away. For *nothing* they threw that away.

But it is true everywhere — whether we are here, or we are in China or we are in Germany, or we are in Spain, or wherever we are — those two basic principles of our politics are uniformly applicable: our government must defend us against pervasive spying by outsiders, and our government must subject listening to the rule of law at home.

To the citizens of the United States a greater responsibility is given because we must act to subject our government to control in the listening it is doing to hundreds of millions and ultimately billions of people around the world. Ours is the government that is projecting immensities of power into the destruction in the world's societies and ours is the government which must be put under democratic control with respect to that listening. It is our principles *in favorem libertatis* which must be the dominant principles in that story.

Freedom has been hunted round the globe. Asia and Africa have long expelled her. Europe has been bullied into treating her like a stranger and England would arrest her at Heathrow if she arrived. The President of the United States has demanded that no

one shall receive the fugitive, and maybe only Dilma Rousseff wants to prepare in time an asylum for mankind.

You heard a lot of stuff from governments around the world in the last two weeks, but not one statement that consisted of "I regret subjecting my population to these procedures." The German Chancellor, though triumphantly reelected, with not a cloud in her political sky, is in no position to say, "I agreed with the Americans to allow forty million telephone calls a day to be intercepted in Germany; I just want them to stop listening to *my* phone!"

The President of the United States is considering the possibility of not listening to thirty-five mobile phones around the world. The other several hundred million people we listen to are stone out of luck.

You understand what a charade this is, of course. The leaders of global societies do not conduct their classified business over their personal mobile phones. Our listening there is not gaining us important military intelligence. The President of the United States is publicly considering not listening to conversations that leaders of other countries have with their *sposi*, their siblings, and their children. But the conversations nine hundred million other people are having with their *sposi*, their siblings, and their children remain fair game. Nobody is talking about that; you're not supposed to think about it.

The listeners are having a political crisis beyond their previous imaginations in the United States. Listeners do not like to appear in the spotlight. Listeners do not like to be visible at all. The NSA and our other listeners have always worked to keep at least one, if not more than one, agency or person between themselves and public scrutiny at all times. Now they have destroyed their credibility with the domestic security industry around the world, which has realized that they have broken their implicit promises about what they would not hack. The global financial industry is overwhelmed with fear at what they've done — at their recklessness in dealing with the crypto that holds the financial system together. The agencies of the United States government they usually count on are fleeing them.

First the National Institutes of Science and Technology comes out and says, "Yes, yes, the NSA corrupted an important computer security standard we published. We're terribly sorry about that, and we're going to fix it," as though it was the first time that had ever happened. And then, as you noticed, two days after we were last here together, the *New York Times* made itself the vehicle for a leak about how the CIA had almost caught Snowden in 2009 and how he was just a common spy after all — until the following weekend, when the CIA denied it. The Agency said, "No, we had no such understanding. Mr. Snowden was attempting to report a security problem in some software." Mr. Snowden clarified the entire story in his interview with Mr. Risen. For the first time in recorded history, the CIA publicly refused to carry water for the listeners.

That was an enormous event, equivalent in scale to the announcement that General Alexander and the chief civilian administrator of the NSA, Mr. Chris Inglis, will retire next March.

But the most terrible thing that has happened to them in the politics of all of this happened over the German Chancellor's manufactured tantrum. When the United

States government's chief executive — the White House itself — wanted the NSA to appear between them and the truth. "Oh, no, we weren't told our people were listening to the German Chancellor's mobile phone." And NSA said, through leaks that are called espionage unless they come from the top, "Yes, of course we told them!" Suddenly the National Security Agency was standing in the full glare of daylight, being asked to take a bullet by the White House and refusing.

We will never have a another moment of similar political disarray on the side that works against freedom. Not only have they made the issue around the world clear to everybody — not only have they have created martyrs in our comrades at Fort Leavenworth, at the Ecuadorian Embassy in London, and at an undisclosed location in Moscow — not only have they lit this fire beyond the point where they can piss it out, but they have lost their armor. They stand before us in the fullness of who they really are. It is up to us to show that we recognize them.

They are, after all, just us — just good patriotic Americans like us. Nothing is wrong with them that an election wouldn't cure. But it will have to be an election to remember — a Parliament of Wonders. And it won't have to be just here.

What they have done is to build a state of permanent war into the Net. Twelve years into a war that will never seem to end, they are making the Net a wartime place forever. We must have peace. We must re-imagine what a Net at peace would look like: cyberpeace. The young people around the world now working on the theory of cyberpeace are doing the most important political work of the later twenty-first century. Because we will now have to provide what democracies provide, which is the end of wars. We have to be willing to declare victory and go home. And when we do, we have to leave behind a Net which is no longer in a state of war, and which no longer uses surveillance to destroy the privacy that founds democracy.

This is a matter of international public law. In the end, this is about something like prohibiting chemical weapons, or land mines — a matter of disarmament treaties, a matter of peace enforcement.

Pervasive surveillance of other peoples' societies is wrong and we must not do it. Our politics, everywhere around the world, are going to have to be based in the restoration of the morality of freedom, which it is the job of democracy to do.

The difficulty is that we have not only our good and patriotic fellow citizens to deal with, for whom an election is a sufficient remedy, but we have also an immense structure of private surveillance that has come into existence, a structure which has every right to exist in a free market but which is now creating ecological disaster, from which governments alone have benefited, and from which people have been rendered far less well off than they think they are, and than they should have been.

You don't need today's *Washington Post* on the subject of the massive interception of information flowing in and out of Google and Yahoo — and soon it will be Facebook and Microsoft's cloud — as we begin to understand what government is doing with "the cloud." You don't need any of that to understand that, at the end of the day, we have to assess not only what the States have done, but also what unregulated enterprise has done, to the ecology of privacy.

We have to consider not only, therefore, what our politics are with respect to the States but also with respect to the enterprises. This is the subject of our talk next time.

For now, we are left attending a puppet show in which the people who are the legitimate objects of international surveillance — namely politicians, heads of state, military officers, and diplomats — are yelling and screaming about how they should not be listened to. As though they were us and had a right to be left alone.

And that, of course, is what they want. They want to confuse us. They want us to think that they are us — that they're not the people who allowed this to happen, who cheered it on, who went into business with it.

The literature of our time has not been deceptive about this. If one reads John le Carré's views about the security industry in Germany under the Global War on Terror (le Carré, as you recall, had his actual experiences as an intelligence officer on behalf of the British government in Germany), if you look at what *A most wanted man* says about the nature of the cooperation between the Germans and the Americans, and its effect on freedom, you will discover that after all everybody really did know — except you.

The purpose of secrecy was to keep you in the dark. The purpose of secrecy was not to prevent the States from knowing what they were doing: their left hands and their right hands knew perfectly well what they were up to.

We're going to have to cope with the problems their deceptions created. Because among the things that our listeners have destroyed is the Internet freedom policy of the United States government. We had a good game that we were playing. But now we have comrades and colleagues around the world — working for the freedom of the Net in dangerous societies — who have depended upon material support and assistance from the United States government, and who now have every reason to be worried and to be frightened.

What if the underground railroad had been constantly under efforts of penetration by the United States government on behalf of slavery?

What if every book for the last five hundred years had been reporting its readers at headquarters?

People talk about this as though it were a matter of the publicity of what we publish rather than the destruction of the anonymity of what we read. We will have to look next time very closely at what commercial surveillance really does and how it really does it in order to understand what our politics have to be. Because there, as here, deception, misdirection — waving the handkerchief brightly over here so you do not see what the other hand is doing — is the whole secret to how it works.

The bad news for the people of the world is you were lied to thoroughly by everybody for nearly twenty years. The good news is that Mr. Snowden has told you the truth.

But if we really believe that the truth will set us free, we had better do it now.

Part III: The Union, may it be preserved

November 13, 2013

Since we were last together, Mr. Albert Gore, Jr. — once Vice President of the United States, and the man who got the most votes in the presidential election of 2000 — said, in a public speech in Montreal, that Mr. Snowden had disclosed evidence of crimes against the United States Constitution.

Senator John McCain — who has never gotten the most votes in a presidential election — immediately came out, and said that General Alexander — whose departure has been scheduled, as we discussed last time — should be fired for allowing Mr. Snowden, who was a mere contractor, access to classified information. This sudden and unprovoked attack by Senator McCain on the business model of Booz Allen Hamilton and many of his campaign contributors was, of course, a beautiful example of the misdirection, misleading, and sheer lying we were talking about last time.

Mr. Gore — who was famously a journalist rather than a lawyer before he went into politics, which may account for his occasional love of truthfulness — was of course exercising layman's privilege in talking about crimes against the United States Constitution, much in the way that liberty has been taken with the law when people attack Mr. Snowden as a "traitor." But Mr. Gore is using layman's privilege. Many of the people who have abused the language with respect to Mr. Snowden are lawyers, and should have known better.

But for all that Mr. Gore was substantially closer to the truth than Senator McCain, it is Senator McCain's comment which leads us closer to the heart of where we need to focus our attention now.

Our remaining time together will be short and in it we must attend to the solutions to some to the problems we have been living with. In order to think about those solutions, we must be sure that we understand the full breadth of the problems. Senator McCain, in referring to the contractors, brought us face to face with the crucial role of the private surveillance market in the world, the data-miners and the listeners of commerce, both those who are officially part of the intelligence establishment and those who aren't. Senator McCain of course knows the vast surveillance-industrial state which has grown up since 2001 — which was so beautifully documented by the Washington Post in its "Top Secret America" series in 2010 — is impossible to imagine, the surveillance behemoth we now have in government cannot be conceived, without the contractors. That's the center of that story. But it is in itself another layer — one might say a superstructure raised atop another structure altogether, one might call a base — which is the great data-mining industry that has grown up in the United States, to surveil the world for profit, in the last fifteen years. It is there that we must pay our central attention before we discuss how to fix things, because there is the center of the problem.

The government abuse of the systems of surveillance and listening which have threatened to fasten the procedures of totalitarianism on everyone in the world without a U.S. passport, this form of pervasive spying on societies which has come into existence, is environmental and ecological crisis brought on by industrial overreaching.

It is not the first, the last, or the most serious of the various forms of environmental crisis brought on in the last two hundred years by industrial overreaching. We

have seen industrial overreaching begin to modify the climate of the whole earth in unexpected and damaging ways. Against that enormity, this is merely an ecological disaster threatening the survival of democracy.

We need to understand the ecological harm done underneath, before we can begin to restrict the listening of government to its appropriate sphere, and abate those violations of the constitution to which Mr. Gore referred.

Now I spoke last time of the way in which we can decompose "privacy," the concepts that we float around under that word, into three more specific parts: First, the problem of secrecy: that is, maintaining our ability to have our messages understood only by those to whom we intend to send them. Second, the problem of anonymity: that is, our interest in maintaining the ability to send and receive messages, which may be public in their content, without always revealing who said and who listened or read what was said. Third, the problem of autonomy, which is the avoidance of coercion, interference, and intervention by parties who have violated either our secrecy or our anonymity and who are using what they have gained by those violations to control us.

I would ask you also — in thinking analytically about this substance, "privacy," whose continuation, I am asserting, is essential to democracy's survival — I would urge you also to consider that privacy is an ecological rather than a transactional substance. This is a crucial distinction from what you are taught to believe by the people whose job it is to earn off you.

Those who wish to earn off you want to define privacy as a thing you transact about with them, just the two of you. They offer you free email service, in response to which you let them read all the mail, and that's that. It's just a transaction between two parties. They offer you free Web hosting for your social communications, in return for watching everybody look at everything, and that, they assert, is a transaction in which only the parties themselves are engaged.

This is a convenient fraudulence — another misdirection, misleading, and plain-lying proposition. Because, as I suggested in the analytic definition of the components of privacy, privacy is always a relation among people. It is not transactional, an agreement between a listener or a spy or a peephole-keeper and the person being spied on.

If you accept this supposedly bilateral offer, to provide email service for you for free as long as it can all be read, then everybody who corresponds with you has been subjected to the bargain, which was supposedly bilateral in nature.

If your family contains somebody who receives mail at Gmail, then Google gets a copy of all correspondence in your family. If another member of your family receives mail at Yahoo, then Yahoo receives a copy of all the correspondence in your family as well.

The idea that this is limited to the automated mining of the mail, to provide advertisements which you may want to click on while you read your family's correspondence, may or may not seem already louche beyond acceptability to you, but please to keep in mind what Mr. Snowden has pointed out to you: Will they, nil they, they are sharing all that mail with power. And so they are helping all your family's correspondence to be shared with power, once, twice, or a third time.

The same will be true if you decide to live your social life in a place where the creep who runs it monitors every social interaction, and not only keeps a copy of everything

said, but also watches everybody watch everybody else. The result will not only be, of course, that you yourself will be subjected to the constant creepy inspection, but also that everybody you choose to socialize with there will be too. If you attract others to the place, you're attracting them to the creepy supervisory inspection, forcing them to undergo it with you, if they want to be your "friend."

The reason that we have to think about privacy the way we think about the other ecological crises created by industrial overreaching is that it is one. It's that we can't avoid thinking about it that way, no matter how much other people may try to categorize it wrongly for us.

This is a particular problem for the lawyers. Because the lawyers are attracted by the shininess of transactional behavior. It gives them benefits and causes them — if they are professors — to lunch, and — if they are practitioners — to dine, in elegance. So they are always delighted to discover a transaction that can be facilitated for a reduction of friction monetized as legal fees. Therefore lawyers are among those around the world most likely to be inclined to imagine that this nonsense about the transactionality of privacy is true. The important element in this is that what is transactional can be consented to, and so we get a lot of law about consent. Which, if correctly understood, is totally irrelevant and indeed fundamentally inappropriate.

We do not, with respect to clean air and clean water, derive the dirtiness of the air and water from the degree of consent. You can't consent to expose your children to unclean or unsafe drinking water in the United States, no matter how much anybody pays you. Because the drinking water must be provided at a socially established standard of cleanliness, which everybody has to meet.

Environmental law is not law about consent. It's law about the adoption of rules of liability reflecting socially determined outcomes: levels of safety, security, and welfare.

When you take a subject which has previously been subject to environmental regulation and you reduce it to transactionality — even for the purpose of trying to use market mechanisms to reduce the amount of pollution going on — you run into people who are deeply concerned about the loss of the idea of a socially established limit. You must show that those caps are not going readily to be lifted in the exhilarating process, the game, of trading.

But with respect to privacy we have been allowed to fool ourselves — or rather, we have allowed our lawyers to fool themselves and them to fool everybody else — into the conclusion that what is actually a subject of environmental regulation is a mere matter of bilateral bargaining. A moment's consideration of the facts will show that this is completely not true.

Of course we acquired this theory not by accident. We acquired this theory because tens of billions of dollars in wealth had been put in the pockets of people who wanted us to believe it.

And on the superstructure that came from that base — that is, fooling us into the belief that privacy was not a subject of environmental concern — environmental devastation was produced by the ceaseless pursuit of profit in every legal way imaginable — which, of course, is more ways than there ought to be, once appropriate ecological restraints either have been lifted or have never been imposed.

Now I'm going to focus my analysis on this point in a single corner of the diagram that one might set forth about the forms of privacy, the nature of the various forms of invasion, and the ways in which unrestrained industrial activity has resulted in catastrophe, upon which government has based its own misdeeds. I'm going to focus only in one corner, which is the one of greatest importance and the one least discussed, namely the way in which this ecological catastrophe has destroyed the anonymity of reading.

There is a tendency, in discussing the privacy catastrophe arising from the behavior of the data-mining behemoths, to suggest that it has something to do with humanity's over-publishing, that the real problem of privacy is that kids are just sharing too darn much.

This is not only a form of misdirection and misleading, it's a form of misdirection and misleading which is especially beautiful, because it hides the truth, both from the people it convinces and from the people who oppose it. It is an all-purpose obscurantist device.

When you democratize media, which is what we are doing with the Net, then obviously people say more — way more — than they were ever able to say before. As when first there was printing, people said more than they could ever say before.

This is not the problem. There may be too much saying or too little: This is to be left, in a free society, to the people who do the saying and the discouraging of saying, all of which is perfectly permissible and about which nobody should do any complaining or do any worse than complaining.

But really what has gone wrong is the destruction of the anonymity of reading, for which nobody has contracted at all.

Because of the way we built the Web — because we gave people programs called "browsers" that everyone could use, but we made programs called "Web servers" that only geeks could use — almost everyone on Planet Earth has never read a Web server log.

This is a great failing in our social education about technology. It's equivalent to not showing children what happens if cars collide and people don't wear seat belts.

We don't explain to people how a Web server log represents the activity of readers, nor how much — if you can aggregate a few hundred million webserver log entries together — you can learn about people, because of what they read — not what they publish, what they read. That you can learn how long they spend on everything they read, how they read it, where they go next, what they do on the basis of what they've just read. If you can collect all that information in the logs, then you are beginning to possess what you ought not to have.

The anonymity of reading is the central, fundamental guarantor of freedom of the mind. Without anonymity in reading, there is no freedom of the mind. Indeed, there is literally slavery.

I don't ask you to accept that statement on my authority. I offer you the authority of a better man than I, who in 1845 published the first of his memoirs, called *A narrative of Frederick Douglass: an American slave.*

Frederick Douglass wrote in that first narrative of his life how his second owner, Sophia Auld, when he was twelve began to teach him letters, and to read a few simple words. But she was vehemently discouraged by her husband Hugh, who told her, when he came to understand what she was doing, "You cannot teach slaves to read, for it will make them uneasy in their slavery, unmanageable and sad." Frederick Douglass said that was the first and deepest abolitionist sermon he had ever heard: "I now understood what had been to me a most perplexing difficulty — to wit, the white man's power to enslave the black man." Thus he began to learn more to read, and when Mrs. Auld, having accepted her husband's direction in the matter, found him reading a newspaper, she tore it away from him lest he become unfit for slavery. Thus he was required, as he tells us, to learn to read in secret.

When hired out to Mr. William Freeland, he taught other slaves to read, until such time as the surrounding slave owners became aware of what he was doing, at which point the mob invaded his Sunday schooling place and beat the people and destroyed the school.

Reading was the pathway, Frederick Douglass wrote, from slavery to freedom. But what if every book and newspaper he touched reported him?

You can go and read almost anything you want, almost any book on Earth, at the headquarters of one of the great American data-mining companies, provided that you let them watch you as you read every page. All books, for free, in the KGB library of Mountain View, California.

Everyone tries to surveil your reading.

If you have a Facebook account which you use, that is you log in from time to time, then not only will Facebook be surveilling every single moment you spend at Facebook — watching what you read, how long you read it, what you do next, where you go to, what you click on from there, etc. — but also every Web page that you touch that has a Facebook "Like" button on it, whether you click the "Like" button or not, will report your reading of that page to Facebook.

And if you go from one page with a Facebook "Like" button on it to another page with a Facebook "Like" button on it, Facebook will calculate how long you spend reading page number one, and so on *ad infinitum* down the chain.

If your newspaper, that you read every day, has Facebook "Like" buttons or similar services' buttons on those pages, then Facebook or the other service watches you read the newspaper, knows which stories you read and how long you spent on them, though you gave Facebook nothing about that at any time.

It's not your publishing which is being surveilled, it is your reading.

Every time you tweet a URL, Twitter is shortening the URL for you. But they are also arranging that anybody who clicks on that URL will be monitored by Twitter as they read.

You are not only helping people know what's on the Web, but also helping Twitter to watch everybody you helped read, so they read over everybody's shoulder everything you recommend.

This isn't transactional, this is ecological. This is an environmental destruction of other people's freedom to read. You are urging them to abandon anonymity under the

guise of helping them to find stuff they want to read. Your activity is designed to help them find things they want to read. Twitter's activity is to disguise the surveillance of the resulting reading from everybody.

The primary actual difficulty, then, has not to do with anything that anybody publishes, or any so called "privacy controls" over who may read what anybody publishes. All of that is a side show, deliberately made complicated, deliberately made controversial, deliberately made full of stuff you're supposed to think about so you never think about the thing that you really ought to know about, which is the surveillance of the reading.

Watch this hand over here in which I wave the flame-colored handkerchief, because otherwise you might be aware of where my left hand is with respect to ... something you consider private.

This is the system that we allowed to grow up so quickly that we did not understand its implications. Which is how ecological crises happen. Because what can be done is done before what will happen next has been thought about. By the time it has been thought about, the people who understood it ain't talking, because they've got an edge, and that edge is directed at you.

Upon this layer of commercial surveillance activity, two things, happen: the complicity and the thievery.

The data-mining companies believed, by and large, with respect to the United States and other governments around the world with whom they deal, that they were merely in a situation of complicity.

Having created unsafe technological structures that mined you, they thought they were merely engaged in quiet — that is to say, undisclosed — bargaining with power over how much of what they had on you they should deliver to others.

This was, of course, a mingled game of greed and fear.

But what the American data-mining giants of the West Coast basically believed, until Mr. Snowden woke them, was that by complicity they had gained immunity from actual thievery.

What sent both Facebook and Google into orbit since we were all last together — or rather, what had come out two weeks ago, on the Wednesday that we were last together — was the news that their complicity had bought them nothing.

Everywhere outside the United States, the United States government had hacked, tapped, stolen its way inside their charmed circle of encryption between themselves and their customers, in order to get to the data after it had been decrypted inside their own houses, their own internal networks, where they did not keep it adequately secure.

Naturally, this bothered the people who had the impression — which Abraham Lincoln so vividly described with respect to his venal Secretary of War Simon Cameron — that "An honest man is a man who, when bought, stays bought."

What they had expected by way of honesty from the American listeners they discovered that they hadn't got at all.

The American listeners had learned their negotiation style from their Soviet counterparts, and their attitude was, "What's ours is ours, and what's yours is negotiable. Unless we steal it first."

Now I do indeed have sympathy for the outraged position of the American data-miners. Most of me feels that they earned the penalty of their complicity, but I am charmed by the naïveté with which they disregarded what we (my comrades and I) told them for twenty years, which was that the listeners are not to be trusted, in any of the things they have said about this.

Like the the world financial industry, they had taken the promises of the American military listeners too seriously. They had believed that there were limits to what power would do, ignoring that power not only had authorization and resources, but also instructions everywhere outside the United States to take anything that it could be, and that the rules regarding the limitations of listening inside the United States under the rule of law had basically been lifted by an administration full of people who were politicizing fear and who were famously engaged in shooting first and asking questions later.

So the problem is that, for the data-miners, the situation is not controllable, just as for the American listeners it is no longer controllable.

And it will only be controllable for us if we bend our attention closely to the environmental nature of the problem that we face, because environmental problems — like climate change, or water pollution, or slavery — are not solved transactionally by individuals.

If you want to get people out of slavery you've got to work together. It takes a Union to destroy slavery.

If you want to solve the problem of the dirty air we breathe, the unclean water that we drink, the changing climate under which we live, we must work together. We will not be able to solve those problems by ourselves.

The essence of the difficulty is Union.

Which, brings us, of course, to another characteristic of the great data-miners of the early twenty-first century, which is that there was no union of any kind around them.

They have become public corporations, but the kinds of environmental issues that we face with them, shareholder democracy has never had the slightest adequate effect in controlling. Though they are publicly-held businesses now, they are remarkably opaque with respect to all that they actually do. They are so valuable that who will kill the goose that lays the golden egg by inquiring whether their business methods are ethical?

A few powerful individuals control all the real votes in these places. Their workforces do not have collective voice. This is important with respect to environmental harms.

Mr. Snowden has been clear all along that the remedy for environmental destruction is democracy and he is correct about that. But Mr. Snowden has also repeatedly pointed out that, in an environment in which workers cannot speak up and there is no collective voice, there is no protection for the public's ability to know.

So now we come to the particular intersection between the destruction of the right to read anonymously and the absence of unions within the organizations that surveil humanity.

When there is no collective voice for those who are within structures that deceive and oppress, then somebody has to act courageously on his own. Someone has to face all the risk for a tiny share of the total benefit that will be reaped by all.

Such a man may be walking the pathway from slavery to freedom. But any such man worthy of the effort will know that he may also be digging his own grave.

When there is no Union, we require heroism. Or we perish for want of what we should have known, that there was neither collective will nor individual courage to bring us.

It takes a Union to end slavery, because a man who decides that the will of the righteous commands us to free slaves will be called a traitor, and they will hang him — more than once.

This is why, when anonymous reading can no longer occur, we imperil the very thing that without Union is the only route to our salvation, while democracy itself strangles in the loop that its security vehicles have drawn around it.

Before Augustus, the Romans of the late Republic knew that the secrecy of the ballot was essential to the people's right.

In every country in the world which holds meaningful elections, Google knows how you're going to vote. It's already shaping your political coverage for you, in your news feed, based upon what you want to read, and who you are, and what you like. Not only does it know how you're going to vote, it's helping to confirm you in your decision to vote that way — unless some other message has been purchased by a sponsor.

Without the anonymity of reading there is no democracy. I mean of course that there aren't fair and free elections, but I mean more deeply than that that there is no such thing as free self-governance.

The crisis of the ecology attacks the root of democracy; Mr. Snowden's point is valid across a bigger world than the world that Mr. Snowden came to talk to us about.

And as we try to turn our attention to what we do about all this, we need to understand it is that ecological crisis we must address, not merely the problem of the power and the daring and the relentlessness of the American military listeners.

And we are still very ill-informed, because there are no unions out there working to raise the ethical issues in the data-miners, and we have too few Snowdens.

The futures of the data-miners are not all the same. Google as an organization has concerned itself with the ethical issues of what it does from the beginning. Mr. Page and Mr. Brin did not stumble on the idea that they had a special obligation not to be evil. They understood the nature of the power implicit in the situation.

We can say for sure that, if we are to be transparent to these companies, then they must be accountable to us. And we can say for sure that it will not be suitable for Google to present to us the proposition that they will do everything they can to protect the secrecy and anonymity of our email except that which is inconsistent with their reading it all themselves.

It is technically feasible for Google to make Gmail into a system which is truly secure and secret for its users. In which mail is encrypted — using public keys in a web of trust — within users' own computers, in their browsers, and in which email at rest at Google is encrypted using algorithms to which the user rather than Google has the relevant keys.

This means donating profit to the world, consistent with the idea that the Net belongs to its users throughout the world — which, in the long run, it is good for Google to be seen not only to believe, but to act upon.

There are many, many, very thoughtful, capable, dedicated people at Google who must choose either doing what is right or naming what is wrong.

The situation at Facebook is different. Facebook is strip-mining human society.

The idea of social sharing, in a context in which the service provider reads everything and watches everybody watch, is inherently unethical.

But we need no more from Facebook than truth in labeling.

We need to no rules, no punishments, no guidelines. We need nothing but the truth.

Facebook should lean in and tell its users what it does.

It should say, "We watch you every minute that you're here. We watch every detail of what you do, what you look at, who you're paying attention to, what kind of attention you're paying, what you do next, and how you feel about it based on what you search for.

"We have wired the Web so that we watch all the pages that you touch that aren't ours, so that we know exactly what you're reading all the time, and we correlate that with your behavior here."

To every parent, Facebook should say, "Your children spend hours every day with us. Every minute of those hours, we spy upon them more efficiently than you will ever be able to."

Only that, just the truth. That will be enough.

But the crowd that runs Facebook, that small bunch of rich and powerful people, will never lean in close enough to tell you the truth.

So I ought to mention that since the last time we were together, it became known that Mr. Zuckerberg has spent thirty million dollars that he got from raping human society on buying up all the houses around his own in Palo Alto — because he needs more privacy.

I rest my case.

We will have a politics that requires of the States — as I said last time — that governments shall protect their people against spying by outsiders and shall subject their listening to the rule of law. We in the United States have a third political obligation, as citizens, which is to prevent our government from using its raw power and resources to subject to the procedures of totalitarianism every other society on Earth besides our own.

But we will have also a politics in the market, a politics of requiring the organizations with whom we deal to treat ethically the ecological substance of human existence. Not only the air, the water, and the land, but the privacy of people and anonymity of reading and the freedom of the mind.

We will require this of them, not casually or doubtfully, but because the opposite is slavery, and we're not going to fool around with that.

Albert Gore is putting pressure on some politicians to tell the truth. He is right that we must have a politics of truthfulness now.

Nine votes in the United States Supreme Court can straighten out what has happened to our law, and there is nothing we need to do about those analysts, who are not bad people, as Mr. Snowden states, other than to hold an election.

But the president of the United States has the only vote that matters concerning the ending of the war.

All of the environmental destruction of privacy which is placed on top of this larger ecological disaster created by industry, all of this spying, is wartime stuff.

A great deal of confusion, to which we shall pay more attention, the last time we are together, has been raised between "data" and "metadata." As though there were a difference and "metadata" were less. I need to explain to you in the simplest way I can why this is nonsense:

Illegal interception of the content of a message breaks your secrecy.

Illegal interception of the metadata of a message breaks your anonymity.

It isn't less, it's just different. Most of the time it isn't less, it's more.

The metadata misdirection is an important part of how we avoid discussing where the iron shackle really is. The anonymity of reading is broken by the collection of metadata.

It isn't the content of the newspaper Mr. Douglass is reading that is the problem, it's that he dares to read it.

The President of the United States can apologize to people for the cancellation of their health-insurance policies, but he cannot merely apologize to the people for the cancellation of the United States Constitution. He must do something.

The President must end this war.

The President must remove the various consequences that flow from the idea that we are at war because there are a few vicious criminals we are pursuing round the globe.

It was wisdom in Thomas Jefferson not to go to war with the Barbary pirates, just to smack them.

It was not wisdom to declare war in the Net, to deprive us of civil liberties under the concept of depriving sanctuary to foreign bad people. It has not been wisdom to protract this war for twelve long years. The wisdom of this President ought to be to say that the war is over.

Because when you're the President of the United States, you also cannot apologize for not being on Frederick Douglass's side.

We have to protect the anonymity of reading.

We have every right to ask, respectfully but insistently, of the President that he shall stop this war. That he shall cease from troubling us with the oppressive consequences of a mere symbolic declaration. That he shall cease from feeding the nightmare of the coalescence of government security with the strip-mining of society. That he shall cease to treat our Net, which belongs to all the people of the world, as the property of the United States listeners, to be hacked, and tapped, and stolen in as necessary from the military point of view.

He must tell the truth: That only peace can sustain freedom, and that indefinitely protracted war leads only to slavery in the end.

We have more to do than that. His work can be done with a word. Ours requires the building of a Union — many Unions.

A man who brings evidence to democracy of crimes against freedom is a hero, and a man who steals the privacy of societies for his profit is a villain. We have sufficient villainy and not enough heroism.

We have to name that difference strongly enough to encourage others to do right.

Mr. Douglass spoke my mind: "I will unite with anyone to do right and with no one to do wrong," he said. In the end, that is how it happened, as it will happen for us.

We have an environmental problem. Like all environmental problems, it has technical, legal, and political components. We must address all of them in their full breadth, in order to bring ourselves to a successful resolution.

It is good that we have fire codes, and it is good that we have rules of liability that make manufacturers responsible if their building materials or their children's clothing goes up at the first lick of flame. It is good that we have building inspectors, so that we try to keep track of who's adding an illegal addition that they might rent out to nineteen or twenty poor defenseless people who might burn to death one night in a fire trap.

All of that is good, but it is very important that we have smoke detectors and fire-extinguishers that people can afford, that they can learn to use, and that will save their families' lives when everything else doesn't work.

We will need technical measures that provide people with inexpensive appliances, that they can actually use, that will help them to avoid being spied on. Large parts of the commercial surveillance structures I have been talking about are easily defeated using technologies commonplace among those who life's work is technological in nature, but largely inaccessible to everybody else. We must popularize it, make it simple, cheap, and easy — and we must help people to put it everywhere.

As we must have political measures appropriate to each where we are and legal measures similarly carefully disposed.

What Mr. Snowden has done with respect to the technological measures is to explain to us precisely what we can use, given where the listeners are in their attempt to subdue everything.

What Mr. Snowden taught us — which is the specific subject of my last lecture — is how to offer people cheap, easy, accessible things that work.

With respect to the politics, he has told us what we should have known ourselves, which is that democracy requires that truth be told to the citizens who vote. He has been restrained in his politics, because he has limited himself to that.

It isn't only Frederick Douglass, but also Thomas Jefferson, who would have a hard time denying Mr. Snowden's propositions. One has to be a lesser politician, I believe, than they to be willing to controvert what Mr. Snowden has said.

And about law. Well, there is lots to say, but the really important part of this, as we shall see next time, is that the United States is plentifully provided with lawyers, good ones, ones who mean to use the rules to protect freedom, ones who have acted, if not precisely with heroism, then at least with courage which deserves much praise.

The former general counsel of Twitter, Mr. Alexander Macgillivray, tried long and hard, and with great conscientiousness and dedication, as we now know, to withstand layers of demand from power that other clients of other lawyers in Silicon Valley rolled over for very easily.

To Mr. Macgillivray, Twitter's former general counsel, much thanks is due.

The Electronic Frontier Foundation, the Electronic Privacy Information Center, my own Software Freedom Law Center — which has helped to sponsor these lectures here — all have roles to play, and they are playing them aggressively in American society. If the rule of law is restored to listening, we will use it well. Not only for the benefit of people in the United States but around the world. Elsewhere, many courageous lawyers have come to gather around projects worthy of everybody's praise and support. In India, the Software Freedom Law Center's sister organization, lead by Ms. Choudhary who is here, are doing wonderful work. We will see elsewhere many courageous lawyers at the forefront.

But we have seen none of these whistle-blowers outside the English-speaking world, nor have they come to us from industry.

It is a special quality of the dying rule of law in the English-speaking world that it encouraged heroism. Because people felt that, bad as the risks were, they were not hopeless. Heroic people believed that courage is contagious, that if people act to reveal the truth, others will follow them towards the light.

Now we must prove them right. Because without Union, without heroism — without a willingness to understand that we must act together, not separately, to preserve freedom — those who serve power with misdirection, misleading, with lies, will get ahead of us. Which must not happen.

Part IV: Freedom's future

December 4, 2013

We must now turn our attention from what Mr. Snowden has taught us concerning the scope of our problem to what, with his assistance, we may do to conceive our responses.

We have seen that, with the relentlessness of military operation, the listeners in the United States have embarked on a campaign against the privacy of the human race. They have — across broad swathes of humanity — compromised secrecy, destroyed anonymity, and adversely affected the autonomy of billions of people.

They are doing this because they have been presented with a mission by an extraordinarily imprudent national government in the United States, which, having failed to prevent a very serious attack on American civilians at home, largely by ignoring warnings, decreed that they were never again to be put in a position where they should have known.

This resulted in a military response, which is to get as close to everything as possible. Because if you don't take as close to everything as possible, how can you say that you knew everything that you should have known?

The fundamental problem was the political, not the military, judgment involved. When military leaders are given objectives, they achieve them at whatever collateral cost they are not prohibited from incurring. That is their job. And if you apply General Curtis LeMay to a situation and you get havoc, well, that's what you called General LeMay in for. General LeMay was correct when he said that, if the United States had lost the Second World War, he and his staff would have been tried for war crimes. From General LeMay's point of view, that meant he was performing his job.

It is not for them, the soldiers and the spies, to determine for themselves when their behavior is incompatible with the morality of freedom. That is why we regard democracy as requiring, among other things that are *sine qua non,* civilian control of military activity. When an especially imprudent U.S. administration abandoned the rule of law with respect to the listeners, leaving behind only a simulacrum in the form of an appointed court operating in secret, the consequences were not for the military listeners to judge for themselves. As we have seen, Mr. Snowden insisted that it was for democracy to impose the limits on that behavior. And democracy — here Mr. Snowden agrees with Mr. Jefferson, and pretty much everybody else who has ever seriously thought about the problem — requires an informed citizenry.

Therefore, Mr. Snowden sacrificed his right to everything that we hold dear — our privacy, our security, our futures — in order to inform the citizens of the United States and the world.

What we are facing, as we have seen, is an environmental calamity, produced by the collateral damage of that military listening, undertaken with relentless efficiency, by people who have more resources than all the rest of the world's listeners put together and whose task was one that they were given by imprudent government authority, which they could legitimately consider as empowering them, indeed instructing them, to steal as close to everything as they could.

Thus they have corrupted science, they have endangered the security of commerce, and they have destroyed the privacy and anonymity of people who live under despotic

governments, who are in danger for what they believe, as a consequence of their destructive behavior. And, as long as it is still called "wartime," as far as they are concerned, they are still doing their jobs.

We have, therefore — as with any other environmental calamity facing the race — no simple answers to any of the questions that are posed. No one thing works. It doesn't even work somewhere, let alone everywhere. On the contrary, we face a problem which, because it is an environmental calamity, calls upon us to perform, as we do at our best, by thinking globally and acting locally — that is to say, by locating the principles that need to be applied with respect to this privacy environmental cataclysm we are living through, and acting in our locales. Each of us must act as befits the role we play and the place we are in, recognizing that collectively we are trying to save freedom of thought and democracy for humanity, which cannot be otherwise saved. Because, as we have seen, pervasive relentless surveillance destroys freedom of thought. And without freedom of thought, all other freedoms are merely privilege conceded by government.

In such a situation we will have, in all the places that we work, political and legal as well as technical measures that we will need to apply — in one sense merely to prevent the problem from growing worse, and in another sense to begin the process of political reversal — as the people of the world signify, in all the places where they are entitled to self-government or the registration of their opinion, that they wish not to be spied on.

Mr. Snowden has shown us the immense complicity of all governments — even those adversarially located with respect to the United States government on many issues — with the United States government's listening. They benefit from the fruits of the research conducted, to the extent that the United States government, by agreement or generosity, is willing to share them. They have turned a blind eye to the corruption of their telecommunications operators, the "infrastructure acquisition" of the Americans, sometimes under intimidation, sometimes under partnership. All of these are relationships which, as Mr. Snowden has shown, extend in many cases back to the period immediately after the end of the Second World War. They have merely grown with time. The technical facilities that were covered by the arrangements went from telegraph to telephone, through rebuilding of the communications network destroyed in Europe by the Second World War. Now they embrace the world-wide "instant-on" Net we currently live within, and will extend, if we do nothing to stop the expansion, further into the one neural system connecting all of humankind in one great big network later in the twenty-first century.

Mr. Snowden has shown, in other words, that everywhere — everywhere where citizens are entitled to a voice in the making of policy — the policies the people want have been deliberately frustrated by their governments. First, they wish to have a government that protects them against outsiders spying. It is the fundamental purpose of government to protect the security of the people on whose behalf it acts, and so it is evident that government must protect citizens against spying from outside, everywhere. And everywhere where citizens are entitled to an expression of their will with respect to the government that conducts policing and national security surveillance at home, it is the will of citizens that such national security surveillance and policing should be subject to the rule of law, under whatever the local institutions for robust protection against government overreaching may be.

Everywhere it is possible to levy those two political requirements by citizens of democracies against their governments. Everywhere. Now. "You are not a government if you are not protecting our security, and our security includes not being spied on by outsiders. And, as you are a State that claims to be governing us under the rule of law, you must also subject your listening, both your national-security listening and your criminal-investigations listening, to legitimate legal review."

In the United States, it will be necessary for us to add a third fundamental political demand to our activity. The United States is not — I mean, we the people of the United States are not — ready to abandon our role as a beacon of liberty to the world. We are not prepared to go out of the business of spreading liberty around the world and to go instead into the business of spreading the procedures of totalitarianism. We never voted for that. The people of the United States do not want to become the secret police of the world. If we have drifted there because an incautious political administration empowered military men to do what military men do — which is full speed ahead, damn the torpedoes — then it is time for the people of the United States to register their conclusive opinion on that subject.

In the meantime, the President of the United States has the only vote necessary to end the war. All of this is possible because it is wartime, or rather because of the myth that it is wartime.

Disregarding the civil liberties of Americans for national-security purposes is possible in wartime only. Declaring that everybody who uses the American telecommunications network who doesn't have our passport is subject to no civil-liberties protection at all is only possible in war time. And the idea that we can abandon the morality of freedom and spread the procedures of totalitarianism around the world in order to achieve security could only be possible in wartime. This cannot be our vision of a peaceful society. The fundamental imprudence was the use of a debatable constitutional privilege to go to war without congressional declaration to create wartime in the United States without end.

The people who did that will be harshly judged by history.

So will the people who refused to stop it.

The President of the United States has one vote and that vote can end the war. Our distinguished and honorable colleagues, the Supreme Court Justices of the United States, have nine votes that can restore the rule of law. No doubt they are reluctant to apply them, for a variety of reasons — some of them I think all of us who are "constitutional thinkers" will agree are serious. But the time is coming when they must act.

All of us who have ever served the federal government, and I am one, have taken an oath to preserve, protect, and defend the Constitution of the United States.

People are going to have to remember that they took that oath.

There come times in the history of the nation when people have to remember that the oath so runs, that it is the protection of the constitutional order of the Union which is the subject of our allegiance.

A clear grasp of that fact has carried us through the most horrible of our national times, and it is what has carried Mr. Snowden to his moment of encounter with the truth.

We are not the only people in the world who have exigent political responsibilities. The government of the United Kingdom must cease to vitiate the civil liberties of its people; it must cease to use its territory and its transport facilities as an auxiliary to American military behavior. And it must cease to deny freedom of the press, and to oppress publishers who seek to inform the world about threats to democracy, while it goes relatively easy on press who spy on murdered girls.

The Chancellor of Germany must stop talking about *her* mobile phone and start talking about whether it is okay to deliver all the telephone calls and SMS in Germany to the Americans — a subject which should be a matter of national discussion in Germany, which the Chancellor is trying not to have by talking instead about her phone. Her charade resembles one of those mobile phone conversations you hear in public all the time, in which people are busy telling one another where they are, but never get down to telling anybody what they really need to do.

Governments that operate under constitutions protecting freedom of expression have to inquire — urgently, as a matter of the morality of freedom in their societies — whether the freedom of expression exists when everything is spied on, monitored, listened to.

In the twentieth century, that would not have been a difficult question, as I pointed out at the beginning of our time together. It would have been regarded as simple and obvious; it is why we were willing to sacrifice tens of millions of lives to destroy what we called fascism and totalitarianism.

I lost a dear friend over the weekend who was imprisoned by the Gestapo in Amsterdam in 1944. It troubles me to think that, with the departure of our dear ones who lived through that time, we might forget what happens when you trifle with the morality of freedom.

We are producing and spreading technology around the world, at the expense of American taxpayers, which is subject to horrendous misuse — to support totalitarianism permanently. That the people doing this want us to believe that, as American leadership, they are trustworthy seems to me utterly irrelevant, having nothing whatever to do with the ethics of equipping any damned despot in the twenty-first century with the opportunity to achieve immortal extent for immorality in power.

In addition to politics, we do have law work to do. In one sense, I have already defined what that law work is: Subjecting things to the rule of law in local courts is lawyers' work. And it is obvious that, if our local politics with global effect is to seek to subject local listening to the rule of law, then lawyers will have to do it. In some places they will need to be extremely courageous; everywhere they will need to be well trained; everywhere they will need our support and our concern.

But it is also clear that subjecting government listening to the rule of law is not the only lawyers' work involved. As we have seen, the relations between the military listeners of the United States, listeners elsewhere in the world, and the big data-mining businesses that have sprung up in the twenty-first century is too complex to be safe for us.

Mr. Snowden's continued revelations have shown the extent to which the data-mining giants in the United States were intimidated, seduced, and also betrayed by the listeners. What has been so angering Google and Facebook is the extent to which the deals they made with the listeners, which they thought conveyed to them protection in return for cooperation, had no such effect at all: The listeners went on hacking, tapping, and stealing from them every way they could. This should not have surprised them, but it did. They apparently didn't think they were dealing with an army in wartime. I don't know why.

And we? We recognize that, at the beginning of the twenty-first century, the network was used to concentrate our data in other people's hands. As we shall see, technological design to deal with the environmental crisis we are living through suggests that we ought to decentralize the data, that we ought not to store it in great big heaps where it is very easy for totalitarian governments and others to go after it.

But, before we come there, we should understand that there are many people managing our data around the world, and they have no responsibility for it. There is lawyers' work to do there too.

In the United States, for example, one of our immediate legislative goals should be to sunset the immunity given to the telecommunication operators for assisting illegal listening in the United States. Immunity was extended by legislation in 2008. Barack Obama, when he was running for President, said that he was going to filibuster that legislation in the United States Senate because it was so Constitutionally ... well, I won't put a word in his mouth. Then, in August 2008, when it became clear that he was going to become the next President of the United States, he changed his mind. Not only did he drop his threat to filibuster the legislation, he flew back from campaigning to Washington, D.C., in order to vote for it in the United States Senate — one of the few things that he felt was worth his time to vote on in the United States Senate as a Presidential candidate in 2008.

We should not argue about whether immunity should have been extended to the operators in the United States; that is not an important question now. We should establish a date certain — say January 21st, 2017, perhaps — after which any telecommunications network operator doing business in the United States that facilitates illegal listening by the United States government should be subject to ordinary civil liability without immunity. No special legislation to make anybody liable for anything is necessary, simply no immunity. An interesting coalition between the human rights lawyers and commercial class-action lawyers would grow up immediately, which would have enormous positive consequences. If the non-immunization extended to non-U.S. network operators that do business in the United States, such for example as Deutsche Telekom, it would have enormous positive consequences for citizens of other countries as well.

In any place where immunity is presently existing and can be withdrawn — recognizing that in most of the places where legal immunity for assisting illegal government listening exists, the citizens never saw it in legislative terms, it was simply done by government in the back behind closed doors in the dark — in any place where the immunity can be withdrawn by legal means, it should be lifted. Helping people to spy on you who have no legal right to do so is conduct that the law, pretty much everywhere, has perfectly well understood carries liability for hundreds if not thousand

of years. There is no reason why we need any new law for that; we just need lawyers to make it work.

Similarly, we need to recognize that this enormous pile of our data in other people's hands is not a problem unknown to the law. On the contrary, the necessary legal principles to deal with it are ones that you encounter every day when you go to the dry cleaner. The English-speaking lawyers refer to this as *bailment.* But really what it means is: If you entrust people with your stuff, they have to take care of it the way that they take care of their own stuff, and if they don't take care of it the way that they take care of their own stuff, then they are liable for their negligence about it.

As a legal historian, I can tell you that reaching this conclusion in the English law required centuries of work and a good deal of backing and forthing and reversal of principles temporarily arrived at, but whether you are a lawyer in the English-speaking world or not, the principles actually spread outward with the Roman commercial law at the beginning of our civilization, roughly at the moment I was talking about some weeks ago, when the Roman Republic was destroyed from inside by a crafty tyrant called Augustus, who assured everybody that they had their old freedoms while taking them away from them, building an intelligence network that made him the best-informed man in the world.

So what we really need to do is to apply the principle of trust in bailment, or whatever the local legal vocabulary is, to all that data which we have entrusted to other people and which they have a responsibility to take care of at least as well as they take care of their own.

Now I share sympathetically the embarrassment of the Google engineers who realized that by lifting all the encryption of other people's data that came to them at the boundaries of Google and then moving it around from one data center to another over fiber-optic lines without re-encrypting it, that they had basically invited the listeners on in. The wolves came in through the back door, after making such a polite deal at the front door — only to accept what Google was prepared to give to them after thinking about it. But in truth, of course, they should know that their computers should be linked by encrypted connections only. I mean, even in my little office we do that.

The real problem here is that the military listeners corrupted our desire to turn the whole Internet into a network that worked that way — with end-to-end encryption — two decades ago, with obscurantist objections, and efforts to delay, and to deny the necessity for end-to-end encryption throughout the Net, because if we built the technology right, everything that moved would be harder for them to steal. We have to come back to that, of course, because we have to do it for ourselves now, whether we are Google, the banks, the hospital, or just our families.

But from the point of view of lawyers' work around the world, there would be an enormous advantage to treating personal data under the rules of bailment, in that we are applying familiar principles concerning our stuff in other people's keeping.

Rules about our stuff in other people's keeping have their being, have the location of their invocation, where the trust is made. If the dry cleaner chooses to move your dry cleaning to another place and then the fire happens, it is not where the fire happened in the place to which they moved your cleaning which determines the liability, it is where they took the clothes from you. The big data-mining giants around the world

play this game of *lex loci server* all the time: "Oh, we are not really in X, we're in California, that's where our computers are."

This is a bad legal habit. It is kind of like eating junk food, these jurisdictional quibbles that are supposed to keep you safe forever. They work until they don't, and then they don't, and then what? We would not actually be doing them a grave disservice if we helped them out of this bad habit, by pointing out that what they really need is legal strategy for dealing with the trust relationships they have with the people that they have, wherever those people are. In the long run it won't do them any real good to deny that they are there. And if we were to apply the correct principles of legal liability to their either adequate or negligent caring for the stuff in their control, we would be doing a sufficient job. It isn't the solution to everything, any more than any principle of liability for environmental harm solves the problem of pollution. But it produces opportunities for productive discussion, which we call "bargaining in the shadow of the law."

We are going to need an international private law of privacy, if you like — that is to say, principles of choice of law around the world which link up the various forms of trust and bailment and "my goods in your hands" and "things I have entrusted to you for you to take care of" in all the various legal systems. This is not international treaty work produced by governments. Governments are not interested: On the contrary, governments are all so far on the other side.

Then there is lawyering to be done in international public law — that is to say, the question of how governments should relate to environmental devastation.

The two most powerful governments in the world, the United States and the People's Republic of China, now fundamentally agree about their policy with respect to threats in the Net. The basic principle is: "Anywhere in the Net there is a threat to our national security, we're going after it."

One of the primary strategists (I refrain from saying apologists) for surveillance in the United States, Mr. Stewart Baker — with whom my acquaintance goes back far too many decades now — Mr. Baker was declaring last week in the United States that it is good for the United States government to keep track of the porn-watching habits of people abroad that it considers to be jihadis who have encouraged attacks on U.S. interests outside the United States.

Mr. Baker said that this was better than murdering them; it was "dropping the truth on their heads." I felt that this was the Internet-enabled equivalent of the old CIA idea to send agents to Cuba with something to put in Fidel Castro's shoes that would make his beard fall out. It's a further example of the nonsense that happens in wartime, but it's also a reminder that the freedom of thought is actually in danger for the most trivial, as well as the most important, of reasons, once this technology of totalitarianism has been spread by us, everywhere.

And so it is reasonable to ask about government-to-government efforts to abate this environmental catastrophe.

The United States and the Soviet Union were in danger of poisoning the world in the 1950s through atmospheric testing of nuclear weapons, and it is to their credit that, in addition to other measures preventing the destruction of the world, they were able to make a bilateral agreement prohibiting atmospheric testing of nuclear weapons.

Which — with occasional toxic efforts by the French to remind everyone that they hadn't agreed to it — pretty much kept people from blowing up nukes in the atmosphere and destroying human civilization by accident.

It is perfectly reasonable to imagine — save only for the fact that the governments have no intention of doing it — an agreement between the United States government and the government of the People's Republic of China to cease turning the human race into a free-fire zone for listening and interfering. But it isn't going to happen this time, as though the Test Ban Treaty had never come into existence.

Now, all of this — all this politics and all this law — unfortunately is slow and uncertain, and at its best it would not arrest the decay of our human environment in this new pervasively spied-upon Net sufficiently, even if it worked fast enough. Without technical solutions, we are fundamentally not going to succeed, just as there is no way to clean up the air and the water or positively affect global climate without technological change.

Everywhere around the world, businesses use software that secures their communications and much of that software is written by us. The "us" I mean here is those coalitions of people sharing technological progress called free software, open-source software, with whom I have worked for decades.

Protocols that implement secure communications used by businesses between themselves and with consumers — HTTPS, SSL, SSH, TLS, OpenVPN, all of these techniques for secure communication in the Net — have been the target of the listeners' interference. Mr. Snowden has shown us very carefully what levels of effort have been applied to the breakage of these fundamental forms of secure communications.

I must point out again that, in stressing this technology, they are courting global financial disaster. If they had succeeded in compromising the fundamental commodity methods by which businesses around the world communicate securely, we would be one catastrophic failure away from global chaos.

Armies in the field, fighting under orders to do whatever it takes, will do things like this. But when the history of this is written, the imprudence of the United States government in having unleashed its military listeners this far is going to be the primary headline. This conduct will appear to the future to represent the same degree of economic recklessness that debasing the Roman coinage did and does: It is a basic threat to the economic security of the world.

The bad news is that they made various kinds of progress: First, they corrupted the science. They covertly affected the making of technical standards in fundamental ways, weakening everyone's security everywhere in order to make their own job easier. (In coming weeks, I will be engaging in more detailed technical discussion about this aspect, with researchers who can speak authoritatively both to what the documents say and to what they mean.)

Second, they have engaged in stealing keys on a level that you can only do when you're the best-financed thieves in the world. Everywhere that encryption keys are baked into hardware, they have been at the bakery. They have collected immense piles of keys, which they keep around, along with superbly skilled teams for stealing them, which they have specially sectored off.

At the beginning of September, when Mr. Snowden's documents on this subject first became public in the *New York Times*, the shock waves of this discovery reverberated all around the industry. They referred to an early version of their "key-recovery" effort to steal systematically keys used for global secure communications by businesses by the code name MANASSAS. Subsequently they much improved it. It was the documentation on the improved second version, which they called BULLRUN, that Mr. Snowden released at the beginning of September.

We can of course conjecture — perhaps we should assume — that even in talking to its own senior leadership, the National Security Agency doesn't tell the whole truth in those documents.

But the very satisfaction they expressed in the expansion of the "key-recovery" — that is, key-stealing — activities, and the subsequent documentation of the extent to which they broke into infrastructure at Google, Facebook, and other places, rather than breaking the SSL encryption between the outside world and the businesses, tends to confirm the most important fact that Mr. Snowden has tried to convey to us, using the Agency's own documents: They prefer — or have chosen by necessity, as the case may be — to steal keys, rather than to break the fundamental crypto that secures the world economy, which is mostly made in the cooperative sector by my clients.

This is the primary inflammatory fact about Mr. Snowden's disclosures, from the perspective of NSA: Telling people what you can and can't read is what listeners would rather die than do. Because as long as nobody knows what you can read you have an aura of omniscience, and if somebody knows what you can't read, then soon you can't read anything anymore. So what Mr. Snowden did was to disclose to us that their advances on our fundamental cryptography were good but not excellent. He showed us that they are gaining ground by brute force, rather than by using some magic rocket ship built in Area 51 that we couldn't compete against.

But Mr. Snowden is also showing us that we have very little time to improve our own crypto, that we have very little time to recover from the harm done to us by standards corruption, and that from now on all of the people who make free-software crypto for everybody to use must assume that they are up against "national means of intelligence," trying to break their technology and socially engineer the subversion of their organizations. In this trade, that is bad news for developers, because that's the big leagues and if you have to play in them every single minute then one mistake is fatal.

Which means that from a technological perspective we have two things we need to do now. The first is that those of use who can must build coalitions to strengthen the basic commodity crypto in the free world and we have to do it right away. The people listening know who they are, and there are youngsters around the world who have great destinies ahead of them, not working under security clearance inside the National Security Agency, but for freedom.

But the second thing we have to do is to change the environment for people so it is safer. This is largely about spreading technologies businesses have been using for a decade and a half now into the lives of ordinary people. Which hasn't happened, you understand.

Cybersecurity is a highly developed professional activity now. Information security officers are smart people doing complicated work, but at the end of the day they set up networks that are safer for the businesses that employ them. We can do that too.

It's as though every factory in the United States had an advanced sprinkler system — smoke detectors, carbon monoxide detectors, sprinklers, high-pressure hoses, fancy fire extinguishers — while everybody's home had no smoke detector, no fire extinguisher, no flame retardant, no nothing.

So what we have to do is to commoditize personal uses of technologies that businesses have already adopted completely, and we need to provide those to people in modalities that don't require anything more than is required to install a smoke detector, hang a fire extinguisher on the wall, talk to your kids about which door to use if the stairs are burning, maybe put a rope ladder in a second-floor window. None of this solves the problem of fire. None of this makes the electrical system safe. It doesn't prevent lightning strikes. It doesn't do anything about the inadequate tax base supporting the fire department. None of that. But if a fire breaks out in your house it will save your child's life.

So we have to do that too. Now, there are projects around the world working on this. FreedomBox is one; there are many others. But I am particularly delighted to see that we are beginning to have commercial competition. I was reading an advertisement for a $49 plug-server-based Tor router last week. Businesses are now aware that the people of the world have not agreed that the technology of totalitarianism should be fastened on every household by the United States and a friendly government in your locality. Not only have the people of the world not agreed to this from a political point of view, they haven't agreed to it from a market point of view either.

If we keep the commodity crypto strong and keep building prototypes of things that would help people to have better privacy, safety, and security in communications, the market will manage. Manufacturers around the world who make a lot of stuff with government inside will also make some stuff with government not inside, because there is money in it.

So, as we pursue our two fundamental responsibilities, the ones that my communities of software makes have pursued relentlessly themselves, if not in a military form, for decades now: Figure out what's good for freedom, make it, share it with people, let other people use it in their businesses, don't impede its improvement. We'll be all right, but only because Mr. Snowden has told us what we can do, what we can't do, what's already lost, and what armor still works. We'll be safe because he did that for us.

Otherwise, the guys at MANASSAS and BULLRUN would keep going, and if they keep going they will reach a point where we have a very hard time reversing what they've done. Because that's what happens with environmental catastrophe: You can't just undo it.

Mr. Snowden is a man conscious of time as well as space and strength. He said in Hong Kong, "I've been a spy all my life." He spied for us, collecting carefully — thoughtfully — for the purpose of making it possible for us to understand and to respond, to save human freedom and democracy. Carefully, thoughtfully, slowly he collected. From the moment he brought that first document into his possession — the

first one that we needed to see and that our government was determined not to let us see — from the moment he had that first document in his possession, he was in mortal danger. Every day he went to work. Every day he did more of what we needed, if we were to sustain ourselves against this runaway military attack on the privacy of humankind.

His courage is exemplary. But he ended his effort because we needed to know *now*. We have to inherit his understanding of that fierce urgency.

In the politics, we must be sure that the leaders of democracies, all of them, know that we have not voted for this. We have not voted elsewhere in the world to be spied on by the Americans without permission.

We in the United States have not voted to cease our role as beacon of liberty to the world. We have not voted to become instead the secret police of everywhere. We have not agreed to be done with the rule of law in the United States — not just with respect to those of us who happen to carry the passport but with respect to everybody who is here.

That's a fundamental commitment; we can't walk away from that. When we walk away from the idea that everyone who is here has constitutional rights, regardless of whether they happen to have a passport, we just reenacted Dred Scott.

Maybe you can do that in wartime. But we have in the past gone to war to prevent that from being the rule in peacetime.

Our politics can't wait about this. Not in the United States, where the war must end. Not around the world, where people have to demand that governments fulfill their basic obligation to protect the security of their people.

If the Chancellor thinks that her mobile phone should not be listened to, I am with her. I am not with her in forgetting about all those other people for whose welfare she is primarily responsible.

At law we have places to go and things to do. Wonderful lawyers around the world, young and old, have work to do, and they're going do it. But they're going to need our support. They're going to need infusions of courage and material welfare, and in some embattled places in the world they're going to need us to be willing to stand with them against physical intimidation and destruction.

We have comrades in Bahrain who were tortured because they carried an iPhone to a demonstration, and it informed on them. We have to do something about that.

As lawyers, we have to recognize that life in a society of pervasive monitoring is not life under the rule of law. This shouldn't be a controversial proposition — but it is.

Technologically, we must shore up — the few thousands of us around the world who make the fundamental technologies that businesses that make hundreds of billions of dollars a year depend upon — we must shore up those technologies against the most skillful attacks that we know of. We must assume that every single one of them has been tried, and that every single thing that could be done to corrupt the fundamental mathematics was done. It's an immense effort — a moon shot of our own. But we must make it.

And then, like that famous U.S. moon shot, we must distribute Tang and "space blankets" and maybe even some more useful stuff to people: aerospace technologies that work at home.

The good news is that many of our laptops already do every single thing we're talking about. I look around this room and I see a lot of people whose technological mechanisms for privacy would be enough, if we multiplied them by a billion people.

We need to decentralize the data, you understand. If we keep it all in one great big pile — if there's one guy who keeps all the email and another guy who does all the social sharing about getting laid — then there isn't really any way to be any safer than the weakest link in the fence around that pile.

But if every single person is keeping her and his own, then the weak links on the outside of that fence get the attacker exactly one person's stuff — which, in a world where listening and spying are governed by the rule of law, might be exactly optimal: One person is the person you can spy on because you've got probable cause.

Email scales beautifully without anybody at the center keeping all of it. We need to make a mail server for people that costs five bucks and sits on the kitchen counter where the telephone answering machine used to be, and that's the end of it. If it breaks, you throw it away.

Decentralized social sharing is harder, but not so hard that we can't do it. Three years ago I called for it. Wonderful work has been done that didn't produce stuff everybody is using, but it's still there: It can't go away, it's free software, it will achieve its full meaning yet.

For the technologically gifted and engaged around the world, this is the big moment, because if we do our work correctly freedom will survive and our grandkids will say: "So what did you do back then?" "I made SSL better."

And if we don't do it ...

Last week in the United States we were celebrating our annual holiday of Thanksgiving. Each year, when we do, we recur to those we call "the Pilgrim Fathers" — religious emigrants from England by way of Holland, who came to Plymouth, Massachusetts in 1620 to worship God and think their thoughts in their own way. The first two years that they spent in what they regarded as an uninhabited country — full of people who knew how to make a living where they did not — were extremely hard. In both winters, there was starvation and many children died.

And in the course of the second winter, of 1621, confreres of theirs — congregationalist Christians in England thinking of emigrating eventually to be with the Plymouth settlement — wrote to them in encouragement, to bear up against the horrible winter they were having. The letter they were writing could not even be delivered to Massachusetts until the spring. The Atlantic Ocean was impassible, but they opened their hearts to their struggling colleagues and they sent their message out into the void, so far away, to such a bitter cold land.

The words they wrote are words that I would speak now to Mr. Snowden: "Be not grievous in your minds," they wrote, "that you have been instrumental in breaking the ice for others. The honor will be yours to the world's end."

We don't often in a human lifetime see a moment of heroism like this, and we forget what we have to do when we've run into it.

Mr. Snowden has nobly advanced our effort to save democracy, and in doing so he has stood on the shoulders of others: of Mr. Assange, Ms. Machon, Mr. Binney, Mr. Drake. The honor will be theirs, but the responsibility is ours. We must see to it that these sacrifices have not been in vain. We have to learn from them.

They have sought a struggle and a hard way. They have endangered themselves and abandoned their futures that we might have the opportunity to govern ourselves in freedom. They have assured us nothing, but they have offered us the chance to assure the generations that come after us that we have given them a world as free as those who came before us gave to us.

And so it is for us, the living — whose lives remain undiminished by the force of oppression, who have not felt the lash — it is for us to finish the work that they have begun.

We must see to it that their sacrifices have meaning — that this nation, and all the nations, shall have a new birth of freedom, and that government of the people, by the people, for the people shall not perish from the earth.

Thank you very much.