Snowden and the Future: Part IV; Freedom's Future

Eben Moglen*

Columbia Law School, December 4, 2013

Good afternoon.

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 Le May 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 US Administration abandoned

*Professor of Law, Columbia Law School; Founding Director, Software Freedom Law Center.

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 future—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. It has been 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—one that they were given by imprudent government authority—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 mortal 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, 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 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 communications 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 communication network destroyed in Europe by the Second World War. Now they embrace the world-wide "instant-on" Net we currently live within, and which we will extend—if we do nothing to stop the expansion, further into the one neural system connecting all of human kind in one great big network later in the 21st 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 debateable 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 do 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 they 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 20th 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 the 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 21st 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 lawyer's 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 21st 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 21st 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 litigators would grow up immediately, which would have very positive consequences. If the non-immunization extended to non-US 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, that 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 tak-

ing 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. 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, 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 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 "Bull Run," 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's 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 technical 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 on 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.

Cyber security 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 commoditize personal uses of technologies that businesses have all ready 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 lighting 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. My FreedomBox project 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 plugserver-based Tor router last week. Businesses are now aware: 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.

So, 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 we must 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 alright, 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 Bull Run they 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 peace time.

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, though we must make it.

And then, like that famous US moonshot, 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 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 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 open

their hearts to their struggling colleagues and they send 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. 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.