Encryption

Privacy under attack: the NSA files revealed new threats to democracy

Eben Moglen

Tue 27 May 2014 06.00 EDT

In the third chapter of his History of the Decline and Fall of the Roman Empire, Edward Gibbon gave two reasons why the slavery into which the Romans had 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 conception of themselves as human beings presupposed freedom. And thus, says Gibbon, for a long time the Romans preserved the sentiments - or at least the ideas - of a 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. As Gibbon wrote, to resist was fatal, and it was impossible to fly.

The power of that Roman empire rested in its leaders' control of communications. The Mediterranean was their lake. Across their European empire, from Scotland to Syria, they pushed roads that 15 centuries later were still primary arteries of European transportation. Down those roads the emperor marched his armies. Up those roads he gathered his intelligence. The emperors invented the posts to move couriers and messages at the fastest possible speed.

Using that infrastructure, with respect to everything that involved the administration of power, the emperor made himself the best-informed person in the history of the world.

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

The empire of the United States after the second world war also depended upon control of communications. This was more evident when, a mere 20 years later, the United States was locked in a confrontation of nuclear annihilation with the Soviet Union. In a war of submarines hidden in the dark below the continents, capable of eradicating human civilisation in less than an hour, the rule of engagement was "launch on warning". Thus the United States valued control of communications as highly as the Emperor Augustus. Its listeners too aspired to know everything.

We all know that the United States has for decades spent as much on its military might as all other powers in the world combined. Americans are now realising what it means that we applied to the stealing of signals and the breaking of codes a similar proportion of our resources in relation to the rest of the world.

The US system of listening comprises a military command controlling a large civilian workforce. That structure presupposes the foreign intelligence nature of listening activities. Military control was a symbol and guarantee of the nature of the activity being pursued. Wide-scale domestic surveillance under military command would have violated the fundamental principle of civilian control.

Instead what it had was a foreign intelligence service responsible to the president as military commander-in-chief. The chain of military command absolutely ensured respect for the fundamental principle "no listening here". The boundary between home and away distinguished the permissible from the unconstitutional.

The distinction between home and away was at least technically credible, given the reality of 20th-century communications media, which were hierarchically organised and very often state-controlled.

When the US government chose to listen to other governments abroad - to their militaries, to their diplomatic communications, to their policymakers where possible - they were listening in a world of defined targets. The basic principle was: hack, tap, steal. We listened, we hacked in, we traded, we stole.

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

> ***Last century we desperately fought and died against systems in which the state listened to every telephone conversation***

The regime that we built to defend ourselves against nuclear annihilation was restructured at the end of the 20th century. In the first place, the cold war ended and the Soviet Union dissolved. An entire establishment of national security repurposed itself. We no longer needed to spy upon an empire with 25,000 nuclear weapons pointed at us. Now we spied on the entire population of the world, in order to locate a few thousand people intent on various kinds of mass murder. Hence, we are told, spying on entire societies is the new normal.

In the second place, the nature of human communication changed. We built a system for attacking fixed targets: a circuit, a phone number, a licence plate, a locale. The 20th-century question was how many targets could be simultaneously followed in a world where each of them required hack, tap, steal. But we then started to build a new form of human communication. From the moment we created the internet, two of the basic assumptions began to fail: the simplicity of "one target, one circuit" went away, and the difference between home and abroad vanished too.

That distinction vanished in the United States because so much of the network and associated services, for better and worse, resided there. The question "Do we listen inside our borders?" was seemingly reduced to "Are we going to listen at all?"

At this point, a vastly imprudent US administration intervened. Their defining characteristic was that they didn't think long before acting. Presented with a national calamity that also constituted a political opportunity, nothing stood between them and all the mistakes that haste can make for their children's children to repent at leisure. What they did - in secret, with the assistance of judges appointed by a single man

operating in secrecy, and with the connivance of many decent people who believed themselves to be acting to save the society – 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 where law no longer provided useful landmarks, but they actually wanted to do it. Their view of the nature of human power was Augustan, if not august. 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 what it knew about the listening. Its decision to censor itself was, like all censorship and self-censorship, a mortal wound inflicted on democracy. We the people did not demand the end at the beginning. And now we're a long way in.

▲ Women working on the Manhattan Project at a secret plant in Oak Ridge, Tennessee, during the second world war – when the enemy was clear. Photograph: Ed Westcott Photograph: Ed Westcott/The Guardian

Our military listeners have invaded the centre of an evolving net, where conscriptable digital superbrains gather intelligence on the human race for purposes of bagatelle and

capitalism. In the US, the telecommunications companies have legal immunity for their complicity, thus easing the way further.

The invasion of our net was secret, and we did not know that we should resist. But resistance developed as a fifth column among the listeners themselves.

In Hong Kong, Edward Snowden said something straightforward and useful: analysts, he said, are not bad people, and they don't want to think of themselves that way. But they came to calculate that if a programme produced anything useful, it was justified.

It was not the analysts' job to weigh the fundamental morality for us.

In a democracy, that task is given by the people to the leaders they elect. These leaders fell - and we fell with them - because they refused to adhere to the morality of freedom. The civilian workers in their agencies felt their failure first. From the middle of last decade, people began to blow whistles all over the field. These courageous workers sacrificed their careers, frightened their families, sometimes suffered personal destruction, to say that there was something deeply wrong.

The response was rule by fear. Two successive US administrations sought to deal with the whistleblowers among the listeners by meting out the harshest possible treatment.

Snowden said in Hong Kong that he was sacrificing himself in order to save the world from a system like this one, which is "constrained only by policy documents". The political ideas of Snowden are worthy of our respect and our deep consideration. But for now it is sufficient to say that he was not exaggerating the nature of the difficulty.

Because of Snowden, we now know that the listeners undertook to do what they repeatedly promised respectable expert opinion they would never do. They always said they would not attempt to break the crypto that secures the global financial system.

That was false.

When Snowden disclosed the existence of the NSA's Bullrun programme we learned that NSA had lied for years to the financiers who believe themselves entitled to the truth from the government they own. The NSA had not only subverted technical standards, attempting to break the encryption that holds the global financial industry together, it had also stolen the keys to as many vaults as possible. With this disclosure the NSA forfeited respectable opinion around the world. Their reckless endangerment of those who don't accept danger from the United States government was breathtaking.

The empire of the United States was the empire of exported liberty. What it had to offer all around the world was liberty and freedom. After colonisation, after European theft, after forms of state-created horror, it promised a world free from state oppression.

Last century we were prepared to sacrifice many of the world's great cities and tens of millions of human lives. We bore those costs in order to smash regimes we called "totalitarian", in which the state grew so powerful and so invasive that it no longer recognised any border of private life. We desperately fought and died against systems in which the state listened to every telephone conversation and kept a list of everybody every troublemaker knew.

> ***Snowden spied on behalf of the human race. As he said, only the American people could decide if his sacrifice was worth it.***

But in the past 10 years, after the morality of freedom was withdrawn, the state has begun 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 and democratic self-governance. Such an argument would be doomed to failure. It is enough to say in opposition that omnipresent invasive listening creates fear. And that fear is the enemy of reasoned, ordered liberty.

It is utterly inconsistent with the American ideal to attempt to fasten procedures of totalitarianism on American constitutional self-governance. But there is an even deeper inconsistency between those ideals and the subjection of every other society on earth to mass surveillance.

Some of the system's servants came to understand that it was being sustained not with, but against, democratic order. They knew their vessel had come unmoored in the dark, and was sailing without a flag. When they blew the whistle, the system blew back at them. In the end - at least so far, until tomorrow - there was Snowden, who saw everything that happened and watched the fate of others who spoke up.

He understood, as Chelsea Manning also 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." So he did what it takes great courage to do 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 as he knew it to tell us things we needed to know. Snowden committed espionage on behalf of the human race. He knew the price, he

knew the reason. But as he said, only the American people could decide, by their response, whether sacrificing his life was worth it.

▲ Listening devices used at Bletchley Park during the second world war. Photograph: Martin Argles Photograph: Martin Argles/The Guardian

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

Even once we have understood, it will be difficult to judge Snowden, because 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. It was right to be right only when all others were right. It was wrong to be right when only people we disagreed with held the views that we were later to adopt ourselves.

Snowden has been quite precise. He understands his business. He has spied on injustice for us and has told us what we require in order to do the job and get it right.

And if we have a responsibility, then it is to learn, now, before somebody concludes that learning should be prohibited.

In considering the political meaning of Snowden's message and its consequences, we must begin by discarding for immediate purposes pretty much everything said by the presidents, the premiers, the chancellors and the senators. Public discussion by these "leaders" has provided a remarkable display of misdirection, misleading and outright lying. We need instead to focus on the thinking behind Snowden's activities. What matters most is how deeply the whole of the human race has been ensnared in this system of pervasive surveillance.

We begin where the leaders are determined not to end, with the question of 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 its people but the world.

This should not actually be a complicated inquiry.

For almost everyone who lived through the 20th century - at least its middle half - the idea that freedom was consistent with the procedures of totalitarianism was self-evidently false. Hence, as we watch responses to Snowden's revelations we see that massive invasion of privacy triggers justified anxiety among the survivors of totalitarianism about the fate of liberty. To understand why, we need to understand more closely what our conception of "privacy" really contains.

Our concept of "privacy" combines three things: first is secrecy, or our ability to keep the content of our messages known only to those we intend to receive them. Second is anonymity, or secrecy about *who* is sending and receiving messages, where the content of the messages may not be secret at all. It is very important that anonymity is an interest we can have both in our publishing and in our reading. Third is autonomy, or our ability to make our own life decisions free from any force that has violated our secrecy or our anonymity. These three - secrecy, anonymity and autonomy - are the principal components of a mixture we call "privacy".

▲ Edward Snowden during an online Q&A. Photograph: ITAR-TASS/Barcroft Media Photograph: ITAR-TASS / Barcroft Media

Without secrecy, democratic self-government is impossible. Without secrecy, people may not discuss public affairs with those they choose, excluding those with whom they do not wish to converse.

Anonymity is necessary for the conduct of democratic politics. Not only must we be able to choose with whom we discuss politics, we must also be able to protect ourselves against retaliation for our expressions of political ideas. Autonomy is vitiated by the wholesale invasion of secrecy and privacy. Free decision-making is impossible in a society where every move is monitored, as a moment's consideration of the state of North Korea will show, as would any conversation with those who lived through 20th-

century totalitarianisms, or any historical study of the daily realities of American chattel slavery before our civil war.

In other words, 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!" misdirection has not been about. If it were up to national governments, the conversation would remain at this phoney level forever.

The US government and its listeners have not advanced any convincing argument that what they do is compatible with the morality of freedom, US constitutional law or international human rights. They will instead attempt, as much as possible, to change the subject, and, whenever they cannot change the subject, to blame the messenger.

One does not need access to classified documents 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. From the early 1990s, the public literature of US defence policy shows, strategic and military planners foresaw a world in which the United States had no significant state adversary. Thus, we would be forced to engage in a series of "asymmetric conflicts", meaning "guerrilla wars" with "non-state actors".

In the course of that redefinition of US strategic posture, the military strategists and their intelligence community colleagues came to regard US rights to communications privacy as the equivalent of sanctuary for guerrillas. They conceived that it would be necessary for the US military, the listeners, to go after the "sanctuaries".

Then, at the opening of the 21st century, a US administration that will go down in history for its tendency to think last and shoot first bought - hook, line and sinker - the entire "denying sanctuary", pervasive surveillance, "total information awareness" scheme. Within a very short time after January 2002, mostly in secret, they put it all together.

The consequences around the world were remarkably uncontroversial. By and large, states approved or accepted. After September 2001, the United States government used quite extraordinary muscle around the world: you were either with us or against us. Moreover, many other governments had come to base their national security systems crucially on cooperation with American listening.

By the time the present US administration had settled into office, senior policymakers thought there was multilateral consensus on listening to other societies: it could not be stopped and therefore it shouldn't be limited. The Chinese agreed. The US agreed. The

Europeans agreed; their position was somewhat reluctant, but they were dependent on US listening and hadn't a lot of power to object.

▲ Teenagers during their induction to the Korean People's Army in Pyongyang, North Korea. Photograph: Eric Lafforgue/Barcroft Media Photograph: Eric Lafforgue / Barcroft Media

Nobody told the people of the world. By the end of the first decade of the 21st century, a gap opened 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 governments themselves. This gap was 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.

Snowden saw what happened to other whistleblowers, and behaved accordingly. His political theory has been quite exact and entirely consistent. He says the existence of these programmes, undisclosed to the American people, is a fundamental violation of American democratic values. Surely there can be no argument with that.

Snowden's position is that efforts so comprehensive, so overwhelmingly powerful, and so conducive to abuse, should not be undertaken save with democratic consent. He has expressed recurrently his belief that the American people are entitled to give or withhold that *informed* consent. But Snowden has also identified the fastening of those programmes on the global population as a problematic act, which deserves a form of moral and ethical analysis that goes beyond mere *raison d'état*.

> ***Hopelessness is merely the condition they want you to catch, not one you have to have***

I think Snowden means that we should make those decisions not in the narrow, national self-interest, but with some heightened moral sense of what is appropriate for a nation that holds itself out as a beacon of liberty to humanity.

We can 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 that, when we talk about the American constitutional tradition with respect to freedom and slavery, we're talking about more than what is written in the law books.

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

These are actually the most significant forms of opposition that we face in doing what we know we ought to do.

In the first place, our struggle to retain our privacy is far from hopeless. Snowden has described to us what armour still works. His purpose was to distinguish between those forms of network communication that are hopelessly corrupted and no longer usable, those that are endangered by a continuing assault on the part of an agency gone rogue, and those that, even with their vast power, all their wealth, and all their misplaced ambition, conscientiousness and effort, they still cannot break.

Hopelessness is merely the condition they want you to catch, not one you have to have.

So far as the other argument is concerned, we owe it to ourselves to be quite clear in response: "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.

We have an American constitutional tradition against general warrants. It was formed in the 18th century for good reason. We limit the state's ability to search and seize to specific places and things that a neutral magistrate believes it is reasonable to allow.

That principle was dear to the First Congress, which put it in our bill of rights, because it was dear to British North Americans; because in the course of the 18th century they learned what executive government could do with general warrants to search everything, everywhere, for anything they didn't like, while forcing local officials to help them do it. That was a problem in Massachusetts in 1761 and it remained a problem until the end of British rule in North America. Even then, it was a problem, because the presidents, senators and chancellors were also unprincipled in their behaviour. Thomas Jefferson, too, like the president now, talked a better game than he played.

This principle is clear enough. But there are only nine votes on the US supreme court, and only they count right now. We must wait to see how many of them are prepared to face the simple unconstitutionality of a rogue system much too big to fail. But because those nine votes are the only votes that matter, the rest of us must go about our business in other ways.

The American constitutional tradition we admire was made mostly by people who had fled Europe and come to North America in order to be free. It is their activity, politically and intellectually, that we find deposited in the documents that made the republic.

But there is a second constitutional tradition. It was made by people who were brought here against their will, or who were born into slavery, and who had to run away, here, in order to be free. This second constitutional tradition is slightly different in its nature from the first, although it conduces, eventually, to similar conclusions.

> ***We face two claims. One says: 'It's hopeless, privacy is gone, why struggle?' The other: 'I'm not doing anything wrong, why should I care?'. These are actually the most significant forms of opposition we face.***

Running away from slavery is a group activity. Running away from slavery requires the assistance of those who believe that slavery is wrong. People in 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 help, because slavery is wrong.

We have now forgotten that in the summer of 1854, when Anthony Burns - who had run away from slavery in Richmond, Virginia - was returned to slavery by a state judge acting as a federal commissioner under the second fugitive slave act, Boston itself had to be placed under martial law for three whole days. Federal troops lined the streets, as 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 and the sailor's clothing that he wore. He had the help of a free black seaman who gave him identity papers. Many dedicated people risked much to help him reach New York.

Our constitutional tradition is not merely contained in the negative rights found in the bill of rights. It is also contained in the history of a communal, often formally illegal, struggle for liberty against slavery. This part of our tradition says that liberty from oppressive control must be accorded people everywhere, as a right. It says that slavery is simply wrong, that it cannot be tolerated or justified by the master's fear or need for security.

So the constitutional tradition Americans should be defending now is a tradition that extends far beyond whatever boundary the fourth amendment has in space, place, or time. Americans 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 14th amendment. We should rather be fighting against the procedures of totalitarianism because slavery is wrong. Because fastening the surveillance of the master on the whole 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.

Snowden has provided the most valuable thing that democratic self-governing people can have, namely information about what is going on. If we are to exercise our rights as self-governing people, using the information he has given us, we should have clear in our minds the political ideas upon which we act. They are not parochial, or national, or found in the records of supreme court decisions 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. Americans should learn from that, and are called upon now to do so.

Knowing what we know, thanks to Snowden, citizens everywhere must demand two things of their governments: "In the first place," we must say to our rulers, "you have a responsibility, a duty, to protect our rights by guarding us against the spying of outsiders." Every government has that responsibility.

It must protect the rights of its citizens to be free from intrusive mass surveillance by other states. No government can pretend to sovereignty and responsibility unless it makes every effort within its power and its means to ensure that outcome.

In the second place, every government must subject its domestic listening to the rule of law. The overwhelming arrogance of the listeners and the foolishness of the last administration has left the US government in an unnecessary hole. Until the last administration unchained the listeners from law, the US government could have held up its head before the world, proclaiming that only its listeners were subject to the rule of law. It would have been an accurate boast.

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

▲ Card indexes of the former East German Stasi secret service are seen in Berlin. Photograph: Jan Bauer/AP Photograph: JAN BAUER/AP

To the citizens of the United States, a greater responsibility is given. The government is projecting immensities of power into the destruction of privacy in the world's other societies. It is doing so without any democratic check or control, and its people must stop it. Americans' role as the beacon of liberty in the world requires no less of us.

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 Britain 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 the Brazilian president, Dilma Rousseff, wants to prepare in time an asylum for mankind.

Political leaders around the world have had much to say since Snowden began his revelations, but not one statement that consisted of "I regret subjecting my own people to these procedures". The German chancellor, though triumphantly re-elected with not a cloud in her political sky, is in no position to say, "I agreed with the Americans to allow 40m telephone calls a day to be intercepted in Germany; I just want them to stop listening to my phone!"

The US listeners are having a political crisis beyond their previous imagining. They do not like to appear in the spotlight, or indeed to be visible at all. Now they have lost their credibility with the cybersecurity industry, which has realised 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. The other US government agencies they usually count on for support are fleeing them.

We will never again have a similar moment of political disarray on the side that works against freedom. Not only have they made the issue clear to everybody - not only have they 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 armour. They stand before us in the fullness of who they really are. It is up to us to show that we recognise them.

What they have done is to build a state of permanent war into the net. Twelve years into a war that never seems to end, they are making the net a wartime place forever. We must reimagine what a net at peace would look like: cyberpeace. Young people around the world now working on the theory of cyberpeace are doing the most important political work of our time. We will now have to provide what democracies provide best, which is peace. We have to be willing to declare victory and go home. When we do, we have to leave behind a net that is no longer in a state of war, a net 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 landmines. A matter of disarmament treaties. A matter of peace enforcement.

> ***What if every book for the past 500 years had been reporting its readers at headquarters?***

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. This structure has every right to exist in a free market, but is now creating ecological disaster from which governments alone have benefited.

We have to consider not only, therefore, what our politics are with respect to the states, but also with respect to the enterprises.

Instead we are still at 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 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.

We must cope with the problems their deceptions created. Our listeners have destroyed the internet freedom policy of the US government. They had a good game so long as they could play both sides. But now we have comrades and colleagues around the world who are working for the freedom of the net in dangerous societies; they have depended upon material support and assistance from the United States government, and they now have every reason 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 past 500 years had been reporting its readers at headquarters?

The bad news for the people of the world is we were lied to thoroughly by everybody for nearly 20 years. The good news is that Snowden has told us the truth.

▲ Our secrets in their hands: one of four server rooms at the Facebook data centre in North Carolina. Photograph: Rainier Ehrhardt/Getty Photograph: ALAN BRANDT/AFP/Getty Images

Edward Snowden has revealed problems for which we need solutions. The vast surveillance-industrial state that has grown up since 2001 could not have been constructed without government contractors and the data-mining industry. Both are part of a larger ecological crisis brought on by industrial overreaching. We have failed to grasp the nature of this crisis because we have misunderstood the nature of privacy. Businesses have sought to profit from our confusion, and governments have taken further advantage of it, threatening the survival of democracy itself.

In this context, we must remember that privacy is about our social environment, not about isolated transactions we individually make with others. When we decide to give away our personal information, we are also undermining the privacy of other people. Privacy is therefore always a relation among many people, rather than a transaction between two.

Many people take money from you by concealing this distinction. They offer you free email service, for example. In return, they want you to let them read all the mail. Their stated purpose is advertising to you. It's just a transaction between two parties. Or, they offer you free web hosting for your social communications, and then they watch everybody looking at everything.

This is convenient, for them, but fraudulent. If you accept this supposedly bilateral offer, to provide email service to you for free as long as it can all be read, then everybody who corresponds with you is subjected to this bargain. 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.

▲ If someone in your family uses Gmail, then Google gets a copy of all your correspondence. Photograph: Boris Roessler/EPA
Photograph: BORIS ROESSLER/EPA

Perhaps even this degree of corporate surveillance of your family's email is too much for you. But as Snowden's revelations showed, to the discomfiture of governments and companies alike, the companies are also sharing all that mail with power - which is buying it, getting courts to order it turned over, or stealing it - whether the companies like it or not.

The same will be true if you decide to live your social life on a website where the creep who runs it monitors every social interaction, keeping a copy of everything said, and also watching everybody watch everybody else. If you bring new "friends" to the

service, you are attracting them to the creepy inspection, forcing them to undergo it with you.

This is an *ecological* problem, because our individual choices worsen the condition of the group as a whole. The service companies' interest, but not ours, is to hide this view of the problem, and concentrate on getting individual consent. From a legal perspective, the essence of transacting is consent. If privacy is transactional, your consent to surveillance is all the commercial spy needs. But if privacy is correctly understood, consent is usually irrelevant, and focusing on it is fundamentally inappropriate.

We do not, with respect to clean air and clean water, set the limits of tolerable pollution by consent. We have socially established standard of cleanliness, which everybody has to meet.

Environmental law is not law about consent. But with respect to privacy we have been allowed to fool ourselves.

> ***We've lost the ability to read anonymously. Without anonymity in reading there is no freedom of mind, there's literally slavery***

What is actually a subject of environmental regulation has been sold to us as a mere matter of bilateral bargaining. The facts show this is completely untrue.

An environmental devastation has been produced by the ceaseless pursuit of profit from data-mining in every legal way imaginable. Restraints that should have existed in the interest of protection against environmental degradation have never been imposed.

There is a tendency to blame oversharing. We are often told that the real problem of privacy is that kids are just sharing too darn much. When you democratise media, which is what we are doing with the net, ordinary people will naturally say more than they ever said before. This is not the problem. In a free society people should be protected in their right to say as much or as little as they want.

The real problem is that we are losing the anonymity of reading, for which nobody has contracted at all.

We have lost the ability to read anonymously, but the loss is concealed from us because of the way we built the web. We gave people programs called "browsers" that everyone could use, but we made programs called "web servers" that only geeks could use - very few people have ever 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 aren't wearing seat belts.

We don't explain to people how a web server log captures in detail the activity of readers, nor how much you can learn about people, because of what and how they *read*. From the logs, you can learn how long each reader spends on each page, how she reads it, where she goes next, what she does or searches for on the basis of what she's just read. If you can collect all that information in the logs, then you are beginning to possess what you ought not to have.

▲ Frederick Douglass, the abolitionist who said reading was the pathway from slavery to freedom. Photograph: J R Eyerman/Time & Life Pictures/Getty Photograph: J. R. Eyerman/Time & Life Pictures/Getty Image

Without anonymity in reading there is no freedom of the mind. Indeed, there is literally slavery. Reading was the pathway, the abolitionist Frederick Douglass wrote, from slavery to freedom. Writing his memoir of his own journey, Douglass recalled that when one of his owners tried to prevent him from reading, "I now understood what had been to me a most perplexing difficulty - to wit, the white man's power to enslave the black man."

But what if every book and newspaper he touched had reported him?

If you have a Facebook account, Facebook is surveilling every single moment you spend there. Moreover, much more importantly, every web page you touch that has a Facebook "like" button on it which, whether you click the button or not, will report your reading of that page to Facebook.

If the newspaper 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: it knows which stories you read and how long you spent on them.

Every time you tweet a URL, Twitter is shortening the URL for you. But it is 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 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. *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.

We allowed this system to grow up so quickly around us that we had no time to understand its implications. By the time the implications have been thought about, the people who understand are not interested in talking, because they have got an edge, and that edge is directed at you.

Commercial surveillance then attracts government attention, with two results that Snowden has documented for us: complicity and outright thievery.

The data-mining companies believed, they say, that they were merely in a situation of complicity with government. Having created unsafe technological structures that mined you, they thought they were merely engaged in undisclosed bargaining over how much of what they had on you they should deliver. This was, of course, a mingled game of greed and fear.

What the US data-mining companies basically believed, or wanted us to believe they believed until Snowden woke them, was that by complicity they had gained immunity from actual thievery. But we have now learned their complicity bought them nothing. They sold us out halfway, and government stole the rest.

▲ The headquarters of the US National Security Agency. Photograph: Trevor Paglen/Rex Photograph: Trevor Paglen/REX

They discovered that what they had expected by way of honesty from the US listeners, the NSA and other agencies, they hadn't got at all. The US listeners' attitude evidently was: "What's ours is ours, and what's yours is negotiable. Unless we steal it first."

Like the world financial industry, the great data-mining companies took the promises of the US military listeners too seriously. That, at any rate, is the charitable interpretation of their conduct. They thought there were limits to what power would do.

Thanks to Snowden, for the data-miners, as for the US listeners, the situation is no longer politically controllable. They have lost their credibility, their trustworthiness, before the world. If they fail to regain their customers' trust, notwithstanding how convenient, even necessary, their services may seem to us, they are finished.

Environmental problems - such as climate change, water pollution, slavery, or the destruction of privacy - are not solved transactionally by individuals.

It takes a union to destroy slavery. The essence of our difficulty, too, is union.

Another characteristic of the great data-miners is that there is no union within or around them.

They are now public corporations, but the union of shareholders is ineffective in controlling their environmental misdoing. These companies are remarkably opaque with respect to all that they actually do, and they are so valuable that shareholders will not 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 companies. Their workforces do not have a collective voice.

Snowden has been clear all along that the remedy for this environmental destruction is democracy. But he has also repeatedly pointed out that, where workers cannot speak up and there is no collective voice, there is no protection for the public's right to know.

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

In every country in the world that holds meaningful elections, Google knows how you are going to vote. It's already shaping your political coverage for you, in your customised 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 much more deeply than that I mean there is no such thing as free self-governance.

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

The futures of the data-miners are not all the same. Google as an organisation has concerned itself with the ethical issues of what it does from the very beginning. Larry Page and Sergey Brin [the founders of Google] did not stumble randomly on the idea that they had a special obligation not to be evil. They understood the dangerous possibilities implicit in the situation they were creating.

It is technically feasible for Google to make Gmail into a system that is truly secure and secret, though not anonymous, for its users.

Mail could be encrypted - using public keys in a web of trust - within users' own computers, in their browsers; email at rest at Gmail could be encrypted using algorithms to which the user, rather than Google, has the relevant keys.

Google would be forgoing Gmail's scant profit, but its actions would be consistent with the idea that the net belongs to its users throughout the world. In the long run it is good for Google to be seen not only to believe, but to act upon, this idea, for it is the only way for it to regain those users' trust. There are many thoughtful, dedicated people at Google who must choose between doing what is right and blowing the whistle on what is wrong.

▲ Mark Zuckerberg wants privacy for his family. Photograph: Kristoffer Tripplaar/Sipa US/Rex Photograph: Kristoffer Tripplaar/Sipa US/REX

The situation at Facebook is different. Facebook is strip-mining human society. Watching everyone share everything in their social lives and instrumenting the web to surveil everything they read outside the system is inherently unethical.

But we need no more from Facebook than truth in labelling. We need 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. We have wired the web with 'like' buttons that inform on your reading automatically."

To every parent Facebook should say: "Your children spend hours every day with us. We spy upon them much more efficiently than you will ever be able to. And we won't tell you what we know about them."

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.

Mark Zuckerberg recently spent $30m (£18m) buying up all the houses around his own in Palo Alto, California. Because he needs more privacy.

So do we. We need to make demands for that privacy on both governments and companies alike. Governments, as I have said, must protect us against spying by other governments, and must subject their own domestic listening to the rule of law. Companies, to regain our trust, must be truthful about their practices and their relations with governments. We must know what they really do, so we can decide whether to give them our data.

> ***The president must end this war in the net, which deprives us of civil liberties under the guise of depriving foreign bad people of sanctuary***

A great deal of confusion has been created by the distinction between data and metadata, as though there were a difference and spying on metadata were less serious.

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.

In particular, the anonymity of reading is broken by the collection of metadata. It wasn't the content of the newspaper Douglass was reading that was the problem - it was that he, a slave, dared to read it.

The president can apologise to people for the cancellation of their health insurance policies, but he cannot merely apologise to the people for the cancellation of the constitution. When you are president of the United States, you cannot apologise for not being on Frederick Douglass's side.

▲ Barack Obama: the president has the only vote that matters concerning the end of the war on privacy. Photograph: Sipa USA/Rex Photograph: Sipa USA/REX

Nine votes in the US supreme court can straighten out what has happened to our law. But the US president has the only vote that matters concerning the ending of the war. All the governmental destruction of privacy that has been placed atop the larger ecological disaster created by industry, all of this *spying* is wartime stuff. The president must end this war in the net, which deprives us of civil liberties under the guise of depriving foreign bad people of sanctuary.

A man who brings evidence to democracy of crimes against freedom is a hero. 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.

We have seen that, with the relentlessness of military operation, the listeners in the US have embarked on a campaign against the privacy of the human race. They have 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 US administration, which - having failed to prevent a very serious attack on civilians at home, largely by ignoring warnings - decreed that it would never again be put in a position where it "should have known".

> ***The UK government must cease to vitiate the civil liberties of its people. It must cease to deny the freedom of the press***

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 explicitly prohibited from incurring. That is why we regard civilian control of the military as a *sine qua non* of democracy. Democracy also requires an informed citizenry.

About this, Snowden agrees with Thomas Jefferson [the chief author of America's Declaration of Independence], and pretty much everybody else who has ever seriously thought about the problem. Snowden has shown us the immense complicity of all governments. He has shown, in other words, that everywhere the policies the people want have been deliberately frustrated by their governments. They want to be protected against the spying of outsiders. They want their own government's national security surveillance activities to be conducted under the independent scrutiny that characterises the rule of law.

In addition, 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 instead into the business of spreading the procedures of totalitarianism. We never voted for that. The people of the US do not want to become the secret police of the world. If we have drifted there because an incautious administration empowered the military, it is time for the people of the United States to register their conclusive democratic opinion.

▲ The German chancellor, Angela Merkel, should focus less on her mobile phone and more on whether it is right to deliver all German calls and text messages to the US. Photograph: Fabrizio Bensch/Reuters Photograph: Fabrizio Bensch / Reuters/REUTERS

We are not the only people in the world to have exigent political responsibilities. The government of the UK 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 misbehaviour. And it must cease to deny freedom of the press. It must stop pressuring publishers who seek to inform the world about threats to democracy, while it goes relatively easy on publishers who spy on the families of murdered girls.

The chancellor of Germany must stop talking about *her* mobile phone and start talking about whether it is OK to deliver all the telephone calls and text messages in Germany

to the US. Governments that operate under constitutions protecting freedom of expression have to inquire, urgently, whether that freedom exists when everything is spied on, monitored, listened to.

In addition to politics, we do have lawyering to do. Defending the rule of law is always lawyers' work. In some places those lawyers 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 are too complex to be safe for us. Snowden's revelations have shown that the US data-mining giants were intimidated, seduced, and also betrayed by the listeners. This should not have surprised them, but it apparently did. Many companies manage our data; most of them have no enforceable legal responsibility to us. There is lawyers' work to do there too.

In the US, for example, we should end the immunity given to the telecommunications operators for assisting illegal listening. Immunity was extended by legislation in 2008. When he was running for president, Barack Obama said that he was going to filibuster that legislation. Then, in August 2008, when it became clear that he was going to become the next president, he changed his mind. Not only did he drop his threat to filibuster the legislation, he interrupted his campaigning in order to vote for immunity.

We need not argue about whether immunity should have been extended. We should establish a date - perhaps 21 January 2017 - after which any telecommunications operator doing business in the US and facilitating illegal listening should be subject to ordinary civil liability. An interesting coalition between the human rights lawyers and commercial class action litigators would grow up immediately with very positive consequences.

> ***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 instead into the business of spreading the procedures of totalitarianism***

If non-immunisation extended to non-US network operators that do business in the United States, such as Deutsche Telekom, it would have enormous positive consequences for citizens of other countries as well. In any country where de facto immunity presently exists and can be withdrawn, it should be lifted.

The legal issues presented by the enormous pile of our data in other people's hands are well-known to all systems of law. The necessary principles are invoked every time you

take your clothes to the cleaners. English-speaking lawyers refer to these principles as the law of "bailment". What they mean is, if you entrust people with your stuff, they have to take care of it as least as well as they take care of their own. If they fail, they are liable for their negligence.

We need to apply the principle of trust in bailment, or whatever the local legal vocabulary is, to all that data we have entrusted to other people. This makes them legally responsible to us for the way they take care of it. There would be an enormous advantage in treating personal data under the rules of bailment or its equivalent.

Such rules are governed by the law where the trust is made. If the dry cleaner chooses to move your clothes to another place where a fire breaks out, it doesn't matter where that fire happened: the relevant law is the law of the place where they took the clothes from you. The big data-mining companies play this game of *lex loci* server all the time: "Oh we are not really in country X, we're in California, that's where our computers are." This is a bad legal habit. We would not be doing them a grave disservice if we helped them out of it.

▲ Nuclear testing on Bikini Atoll: the US and USSR eventually agreed to ban such tests. Photograph: US air force Photograph: US Air Force - digital version c/ US Air Force - digital version

Then there is lawyering to be done in international public law. We must hold governments responsible to one another for remedying current environmental devastation.

The two most powerful governments in the world, the US and 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 to attack it."

The US and the Soviet Union were in danger of poisoning the world in the 1950s through atmospheric testing of nuclear weapons. To their credit, they were able to make a bilateral agreement prohibiting it.

The US and the government of China could agree not to turn the human race into a free-fire zone for espionage. But they won't.

> ***In any country where de facto immunity presently exists and can be withdrawn, it should be lifted***

We must pursue legal and political redress for what has been done to us. But politics and law are too slow and too uncertain. Without technical solutions we are 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, businesses use software that secures their communications and much of that software is written by us. The "us" I mean here is those communities sharing free or 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 etc) have all been the target of the listeners' interference.

Snowden has documented their efforts to break our cryptography.

The US listeners are courting global financial disaster. If they ever succeed in compromising the fundamental technical methods by which businesses communicate securely, we would be one catastrophic failure away from global financial chaos. Their conduct will appear to the future to be as economically irresponsible as the debasing of the Roman coinage. It is a basic threat to the economic security of the world.

The bad news is that they have made some progress towards irremediable catastrophe. First, they corrupted the science. They covertly affected the making of technical standards, weakening everyone's security everywhere in order to make their own stealing easier.

Edward Snowden in Moscow after revealing the scale of state surveillance. Photograph: AP Photograph: Uncredited/AP

Second, they have stolen keys, as only the best-financed thieves in the world can do. Everywhere encryption keys are baked into hardware, they have been at the bakery.

At the beginning of September when Snowden's documents on this subject first became public, the shock waves reverberated around the industry. But the documents released also showed that the listeners are still compelled to steal keys instead of breaking our locks. They have not yet gained enough technical sophistication to break the fundamental cryptography holding the global economy together.

Making public what crypto NSA can't break is the most inflammatory of Snowden's disclosures from the listeners' perspective. As long as nobody knows what the listeners cannot read, they have an aura of omniscience. Once it is known what they cannot read, everyone will use that crypto and soon they cannot read anything any more.

Snowden has disclosed that their advances on our fundamental cryptography were good but not excellent. He is also showing us that we have very little time to improve our own cryptography. We must hurry to recover from the harm done to us by technical standards corruption. From now on, the communities that make free software crypto for everyone else must assume that they are up against "national means of intelligence". In this trade, that is bad news for developers, because that's the big leagues. When you play against their opposition, even the tiniest mistake is fatal.

> ***It's as though every factory in our society had an advanced fire safety system - while everybody's home had nothing***

Second, we must change the technical environment so it is safer for ordinary people and small businesses. This is largely about spreading technologies big businesses have been using for a decade and a half. Far too little has so far happened along these lines. It's as though every factory in our society had an advanced fire safety system – smoke detectors, carbon monoxide detectors, sprinklers, high pressure hoses, fancy fire extinguishers – while everybody's home had nothing.

We must commoditise personal uses of the communication security and privacy technologies that businesses have already adopted. This has to be as simple as installing a smoke detector, hanging a fire extinguisher on the wall, talking to your kids about which door to use if the stairs are burning, or even putting a rope ladder in a second-floor window. None of this solves the problem of fire. But if a blaze breaks out, these simple measures will save your child's life.

There are many software projects and startup companies working on these measures. My FreedomBox is one such non-profit project. But I am particularly delighted to see we are beginning to have commercial competition. Businesses are now aware: the people of the world have not agreed that the technology of totalitarianism should be fastened on every household. If the market offers them good products that make this spying harder, they will buy and use them.

> ***We must commoditise personal uses of the communication security and privacy technologies that businesses have already adopted. If the market offers them good products that make this spying harder, they will buy and use them.***

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

Our politics can't wait. Not in the US, where the war must end. Not around the world, where people must demand that governments fulfil the basic obligation to protect their security.

We need to decentralise the data. If we keep it all in one great big pile - if there's one guy who keeps all the email and another guy who manages all the social sharing - then there isn't really any way to be any safer than the weakest link in the fence around those piles.

But if everyone is keeping her and his own, then the weak links on the outside of any fence get the attacker exactly one person's stuff. Which, in a world governed by the rule of law, might be optimal: one person is the person you *can* spy on because you've got probable cause.

Email scales beautifully without anybody at the centre 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. If it breaks, you throw it away.

Decentralised social sharing is harder, but not so hard that we can't do it. 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?" The answer could be: "I made SSL better."

Snowden has nobly advanced our effort to save democracy. In doing so he stood on the shoulders of others. The honour will be his and theirs, but the responsibility is ours.

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.

• This essay is built from the "Snowden and the Future" talk series delivered at Columbia Law School, which is available at snowdenandthefuture.info. It is released under the CC-BY-SA licence.

comments (199)

Sign in or create your Guardian account to join the discussion.