The Guardian

Interview

Edward Snowden interview - the edited transcript

Alan Rusbridger and Ewen MacAskill

The whistleblower speaks to Alan Rusbridger and Ewen MacAskill about life in Russia, the NSA culture, his time there and the future of communication . I, spy: Edward Snowden in exile

Fri 18 Jul 2014 21.00 BST

EDWARD SNOWDEN ON ...

His time in Hong Kong

That whole period was very carefully planned and orchestrated. There was no risk of compromise. I could have been screwed, but the fact that transmissions to journalists would be intercepted, that wasn't possible at all, unless the journalist intentionally passed this to the government.

And I didn't cover my traces. I only tried to avoid being detected in advance of travel, I didn't want to be interdicted, but on the other side I wanted them to know where I was at. I wanted them to know. But because of that they would immediately go: "All right, this guy isn't where he says he's supposed to be. He's supposed to be getting medical treatment. Why the hell is he in Hong Kong?" And I didn't want them to get ahead of the story and basically try to spin the whole spy story.

[Snowden wanted the revelations to be published as fast as possible.] So I was very concerned about all these delays. You've got to remember I knew nothing of the press. I'd never talked to a journalist … I was a virgin source basically.

It was a nervous period. You have no idea what the future's going to hold and I was all right because I knew things would get out but I wanted them to get out in the best way, and that was [why] I didn't want any mistakes. It was what I called the zero fuck-ups policy…

Why he made sure the documents were spread among different countries

It's that concept of herd immunity. They run cover for the others. And particularly once you start splitting them over jurisdictions and things like that it becomes much more difficult to subvert their intentions. Nobody could stop it.

But as an engineer, and particularly as somebody who worked in telecoms and things like that on these systems, the thing that you're always terrified of when you're thinking about reliability is SPOFs - Single Point Of Failure, right?

This was the thing I told the journalists: "If the government thinks you're the single point of failure, they'll kill you."

Why he did not go straight to Ecuador rather than Hong Kong

So this is the thing that nobody realises. They think there was some masterplan to get out safely and avoid all consequences. That's what Hong Kong was all about. But it wasn't. The purpose of my mission was to get the information to journalists. Once I had, that I was done.

That's why I was so peaceful afterwards, because it didn't matter what happened … Going to Ecuador and getting asylum there, that would have been great … And that would have just been a bonus. The fact that I've ended up so secure is entirely by accident. And as you said, it probably shouldn't have happened. If we have anybody to thank, it's the state department. The whole key is, the state department's the one who put me in Russia.

The past year

It's been unexpected and challenging but it's been encouraging. It's been energising to see the reaction from the public. It's been vindicating to see the reaction from lawmakers, judges, public bodies around the world, civil liberties activists who have said it's true that we have a right to at least know the broad outlines of what our government's doing in our name and what it's doing against us.

Being able to be a part of that, even if it's a small part, has been, I think, the most rewarding work of my life.

The White House investigated those programs [which allowed mass surveillance] on two separate occasions and on both occasions found that they had no value at all, and yet, while those panels recommended that they be terminated, when it actually came to the White House suggesting action to legislators, the legislators said: "Well, let's not end these programs. Even though they've operated for 10 years and never stopped any imminent terrorist attacks, let's keep them going."

Life at the NSA

I began to move from merely overseeing these systems to actively directing their use. Many people don't understand that I was actually an analyst and I designated individuals and groups

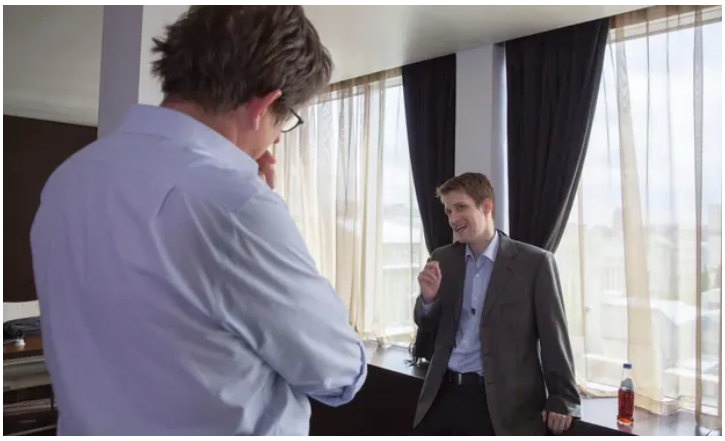
for targeting.

I was exposed to information about the previous programs like Stellar Wind [used during the presidency of George W Bush] for example. The warrantless wire-tapping of everyone in the United States, including their internet data - which is a violation of the constitution and law in the United States - did cause a scandal and was ended because of that.

When I saw that, that was really the earthquake moment because it showed that the officials who authorised these programs knew it was a problem, they knew they didn't have any statutory authorisation for these programs. But instead the government assumed upon itself, in secret, new executive powers without any public awareness or any public consent and used them against the citizenry of its own country to increase its own power, to increase its own awareness.

We constantly hear the phrase "national security" but when the state begins ... broadly intercepting the communications, seizing the communications by themselves, without any warrant, without any suspicion, without any judicial involvement, without any demonstration of probable cause, are they really protecting national security or are they protecting state security?

What I came to feel - and what I think more and more people have seen at least the potential for - is that a regime that is described as a national security agency has stopped representing the public interest and has instead begun to protect and promote state security interests. And the idea of western democracy as having state security bureaus, just that term, that phrase itself, "state security bureau", is kind of chilling.



Snowden revealed going to Hong Kong was not part of a masterplan, adding the state department stranded him in Russia. Photograph: Alex Healey

So when we think about the nation we think about our country, we think about our home, we think about the people living in it and we think about its values. When we think about the state, we're thinking about an institution.

The distinction there is that we now have an institution that has become so powerful it feels comfortable granting itself new authorities, without the involvement of the country, without the involvement of the public, without the full involvement of all of our elected representatives and without the full involvement of open courts, and that's a terrifying thing - at least for me.

Generally, it's not the people at the working level you need to worry about. It's the senior officials, it's the policymakers who are shielded from accountability, who are shielded from oversight and who are allowed to make decisions that affect all of our lives without any public

input, any public debate, or any electoral consequences because their decisions and the consequences of the decisions are never known.

Because of the advance of technology, storage becomes cheaper and cheaper year after year and when our ability to store data outpaces the expense of creating that data, we end up with things that are no longer held for short-term periods, they're held for long-term periods and then they're held for a longer term period. At the NSA for example, we store data for five years on individuals. And that's before getting a waiver to extend that even further.

You have a tremendous population of young military enlisted individuals who, while that's not a discredit to them, ... may not have had the number of life experiences to have felt the sense of being violated. And if we haven't been exposed to the dangers and risks of having our privacy violated, having our liberties violated, how can we expect these individuals to reasonably represent our own interests in exercising those authorities?

The Stasi

No system of mass surveillance has existed in any society that we know of to this point that has not been abused. When we look at the German Stasi for example, they were a state security bureau set up to protect their nation, to protect the stability of their political system, which they considered to be under threat. They were ordinary citizens like anyone else. They believed they were doing the right thing, they believed they were doing a good thing. But when we look at them in historic terms, what were they doing to their people? What were they doing to the countries around them? What was the net impact of their mass indiscriminate spying campaigns? And we can see it more clearly.

The relationship between the NSA and telecom and internet companies

Unusually hidden even from people who worked for these agencies are the details of the financial arrangements between [the] government and the telecommunication service providers. And we have to ask ourselves, why is that? Why are their details of how they're being paid to collaborate with [the] government protected at a much greater level than for example the names of human agents operating undercover, embedded with terrorist groups?

Nighttime aerial picture of the National Security Agency HQ in Maryland, US. Photograph: Trevor Paglen/REX

So the way Prism [the program that deals with the relationship between the NSA and the internet companies] works is agencies are provided with direct access to the contents of the server at these private companies. That doesn't mean the companies can, or the intelligence agencies can, let themselves in. What it means is Facebook is allowing the government to get copies of your Facebook messages, your Skype conversations, your Gmail mailboxes, things like that.

It distinguishes it from where the government is creating its own access – so called upstream operations – where they sort of tap the backbones where these communications cross and they try to take them in transit. Instead they go to the company and they say: "You're going to give us this. You're going to give us that. You're going to give us that." And the company gives them all of this information in a cooperative relationship.

If Facebook is going to hand over all of your messages, all of your wall posts, all of your private photos, all of your private details from their server the government has no need to intercept all of the communications that constitute those private records.

Why governments don't like encryption

The most important sort of law enforcement investigation capabilities and intelligence collection capabilities we have are capabilities that are not going away, regardless of whether they're … in the press, and that is targeted computer exploitation. … You've got a global network that's geographically distributed in basically every country around the world, underneath all the world's oceans.

And the government is saying that we need to be able to intercept all of these communications … And because of this they don't like the adoption of encryption. They say encryption that protects individuals' privacies, encryption that protects the public's privacy broadly as opposed to specific individuals, encryption by default, is dangerous because they lose this midpoint communication, this midpoint collection.

The reality is every communication comes from an originating point and it ends up at a destination point. And these two points are computers, they're devices, they're cell phones or laptops and they can be hacked. They can be exploited, which gives law enforcement agencies and intelligence agencies direct access to those systems to be able to read those communications.

On NSA culture, sharing sexually compromising material

When you're an NSA analyst and you're looking for raw signals intelligence, what you realise is that the majority of the communications in our databases are not the communications of targets, they're the communications of ordinary people, of your neighbours, of your neighbours' friends, of your relations, of the person who runs the register at the store. They're the most deep and intense and intimate and damaging private moments of their lives, and we're seizing [them] without any authorisation, without any reason, records of all of their activities – their cell phone locations, their purchase records, their private text messages, their phone calls, the content of those calls in certain circumstances, transaction histories – and from this we can create a perfect, or nearly perfect, record of each individual's activity, and those activities are increasingly becoming permanent records.

Snowden argues all internet communication should be encrypted so people can avoid being 'electronically naked'. Photograph: Anatolii Babii/Alamy

Many of the people searching through the haystacks were young, enlisted guys and ... 18 to 22 years old. They've suddenly been thrust into a position of extraordinary responsibility where they now have access to all your private records. In the course of their daily work they stumble across something that is completely unrelated to their work, for example an intimate nude photo of someone in a sexually compromising situation but they're extremely attractive. So what do they do? They turn around in their chair and they show a co-worker. And their co-worker says: "Oh, hey, that's great. Send that to Bill down the way." And then Bill sends it to George, George sends it to Tom and sooner or later this person's whole life has been seen by all of these other people. Anything goes, more or less. You're in a vaulted space. Everybody has sort of similar clearances, everybody knows everybody. It's a small world.

It's never reported, nobody ever knows about it, because the auditing of these systems is incredibly weak. Now while people may say that it's an innocent harm, this person doesn't even know that their image was viewed, it represents a fundamental principle, which is that we don't have to see individual instances of abuse. The mere seizure of that communication by itself was an abuse. The fact that your private images, records of your private lives, records of your intimate moments have been taken from your private communication stream, from the intended recipient, and given to the government without any specific authorisation, without any specific need, is itself a violation of your rights. Why is that in the government database?

I'd say probably every two months you see something like that happen. It's routine enough, depending on the company you keep, it could be more or less frequent. But these are seen as the fringe benefits of surveillance positions.

Why the NSA auditing is inadequate

A 29-year-old walked in and out of the NSA with all of their private records. What does that say about their auditing? They didn't even know.

People talk about things that they shouldn't have done as if it's no big deal because nobody expects any consequences. Nobody expects to be held to account. There are no auditors who go into your space and see things other than your own friends. When you're auditing yourselves, what are the real consequences to be expected?

The sharing of ordinary people's intimate photos would happen every couple of months, Snowden told the Guardian. Photograph: Alex Healey

The reality of working in [the] intelligence community is you see things that are deeply troubling all the time. I raised concerns about these programs regularly and widely, [to] more than 10 discreet colleagues that I have worked with - and that's both laterally and vertically in my work. I went to [them] and I showed [them] these programmes and said: "What do you think about this? Is this unusual? How can we be doing this? Isn't this unconstitutional? Isn't this a violation of rights?" and "Why are we intercepting more American communications than we're intercepting Russian communications?"

The people that are staffing these intelligence agencies are ordinary people, like you and me. They're not moustache-twirling villains that are going, "ah ha ha that's great", they're going: "You're right. That crosses a line but you really shouldn't say something about that because it's going to end your career."

We all have mortgages. We all have families. And when you're working for a national security system that has these official secrets acts, that means even if you go to a chosen representative of Congress, a representative chosen by a reporter as opposed to a representative chosen by the intelligence community responsible for the wrongdoing to begin with, you can be prosecuted for it. And even if you're not prosecuted for it, you can lose your job over it.

I was a private contractor as opposed to a direct employee of the National Security Agency. And that meant that what few whistleblower protections we have in the United States did not apply to me. I could have been fired and [would have] had no recourse against the retaliation. I could have been imprisoned. And everybody who works for these agencies, they're all aware of that.

Thomas Drake, an American who exposed widespread lawlessness ... [he was a senior NSA employee who raised concerns about agency programs and their impact on privacy] ... rather than having those claims investigated, rather than having the wrongdoing remediated, they launched an investigation against him and ... all of his co-workers.

They pulled them out of the shower at gunpoint, naked, in front of their families. They seized all of their communications and electronic devices, they interrogated them all, they threatened to put them in jail for life, for years and years and years, decades, and they destroyed their careers.

"The public should not know about these programmes. The public should not have a say in these programmes and, for God's sake, the press had better not learn about these programmes or we will destroy you."

The NSA's British partner, GCHQ, and whether it is worse

Their respect for the privacy right, their respect for individual citizens, their ability to communicate and associate without monitoring and interference is not strongly encoded in law or policy. And the result of that is that citizens in the United Kingdom and citizens around the world who are targeted by the United Kingdom, by the UK government, by UK systems, by UK authorities, they're at a much greater risk than they are in the United States.

GCHQ has a much lighter oversight regime than it should – by its own admission, said Snowden. Photograph: Barry Batchelor/PA

You've got their own admission in their own documents that "we've got a much lighter oversight regime than we should have", full stop. That's what they're talking about. They enjoy authorities that they really shouldn't be entitled to. And the problem with that is, when you have an unrestrained intelligence agency that's not being well overseen, that's not accountable to the public, they're going to go further than they need to. They're going to overreach. They're going to implement systems and policies and target people who are not necessary to target.

Tempora [GCHQ's internet surveillance program] is really proof ... that GCHQ has much less strict legal restrictions than other western government intelligence.

The UK government may publicly say, "We have very strict regulations. There's a broad oversight. There's intense accountability for all of these officials operating these programs". Their own private documents, classified documents they never expect the public to see, say something very different, which is, "We have a very light oversight regime compared to all other western countries".

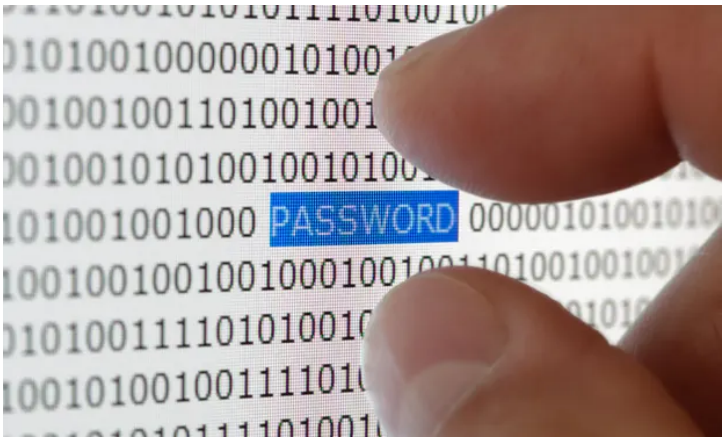
And what that means is UK citizens and UK intelligence platforms are used as a testing ground for all of the other five eyes partners - that's the UK, Canada, the United States, Australia, New Zealand.

This experimental approach at how we collect intelligence, [while] at the same time we keep the public unaware of how we do it, leads to a very unusual situation. Instead of having a signals intelligence system driven by the need to use its authorities only where necessary and only in the measure that is proportionate to the threat, we get a technological approach where they go, "What can we do?" as opposed to, "What do we need to do?".

Hearing the British government wanted to destroy the Guardian's hard drives

First off, I have to admit I kind of clapped my hands. This is stupid. I was shocked that the UK government would go so far for so little. It should have been obvious to anyone who works with data or journalism, or anybody in these intelligence agencies that you can't grind hard disks.

You know, you can't grind data out of existence when we have a global interconnected internet, and particularly when ... the journalists who were on the ground were still out there. And yet they did it. It seemed like a clear intent to intimidate the press into pulling back and not reporting. And I think that was why it was inappropriate but tremendously beneficial for the public conversation because they gave everyone who was concerned about the abuses of power a clear and specific example.



Snowden explained that governments don't like encryption as it makes surveillance that much harder. Photograph: Alamy

In what kind of country do government agents basically bust into newsrooms and demand the destruction of journalistic material? Hopefully that's an event that we won't see happen again.

Metadata

Metadata is contrasted typically against content. People think about metadata being the details of the call - when you made the call, who the call was to, when it happened, how long it occurred for - versus the content of the call, which is what you said. As an analyst, nine times out of 10, you don't care what was said on the phone call till very late in the investigative chain. What you care about is the metadata because metadata does not lie.

People lie in phone calls when they're involved in real criminal activity. They use code words. They talk round it. You can't trust what you're hearing but you can trust the metadata. That's the reason that metadata is often more intrusive.

Metadata can be analogised to the details that a private eye ... produces in the course of their investigation. For example, the private eye might follow you to a diner where you meet a friend, you meet a lover. They see who you meet, they see where you met, they see when you went there and they may even know the broad details of the topics of your conversation, but they won't have gotten the full content. They won't have gotten close enough to expose themselves and hear everything you've said.

What's happened with these programmes is governments in the United Kingdom, for example, the United States and other western governments, as well as much less responsible governments around the world, have taken it upon themselves to assign private eyes to every citizen in their country and around the world to the best of their ability. It happens automatically, pervasively, and it's stored on databases, whether or not it's needed.

Germany

I think it's unfortunate that we see in a number of states - and this is particularly well represented in western Europe - [that] the priorities of governments seem to be very distinct from the desires of the public. I think it's unfortunate when, for example, in Germany evidence has revealed that the NSA is spying on millions of German citizens ... and that's not a scandal. But when Angela Merkel's cell phone is listened [in] on and she herself is made a victim, suddenly it changes relations.

We shouldn't elevate senior officials. We shouldn't elevate leaders above the average citizen because, really, who is it that they're working for? You know the public interest is the national interest. You know the priorities of the NSA should not take precedence over the needs of the German population.

A consensus is growing that the status quo is no longer tenable, that things must change and the public has to have a say in the way the government operates its surveillance apparatus and where the lines are drawn on the boundaries of our rights.

I think it's surprising in Germany that they've asked for me to testify as a witness and aid their investigation into mass surveillance but at the same time they've barred me from entering Germany. That's led to an extraordinary situation where the search for truth has been subordinated to political priorities ... I think it does a disservice to the broader public. ... That's probably too political. I hate politics. Really, I mean, this is not me, you know. I hope you guys can tell the difference.

US-German relations were left strained by claims Angela Merkel's phone had been tapped by the NSA. Photograph: Sean Gallup/Getty Images

Compromising the security of the web itself

A back door in a communications system, in an internet system, in an encryption standard is basically a secret method of getting around the security of those communications. It's a way of subverting all of the privacy claims, all of the security claims that a company or a standard makes to the people who use a product or service.

The danger of building back doors like that, for example the Bullrun program where the NSA and GCHQ were shown to be collaborating and weakening the encryption standards that the entire internet relies on, means that when you're accessing your bank account online there could be a secret weakness there that allows our western governments' security services to monitor your bank details.

What people often overlook is the fact that when you build a back door into a communication system that back door can be discovered by anyone around the world. That can be a private individual, that can be a security researcher at a university, but it can also be a criminal group. It can also be a foreign intelligence agency but, say, the NSA's equivalent in a deeply irresponsible government in some foreign country. And now that foreign country can scrutinise not just your bank records, not just your private transactions but your private communications all around the internet and in every institution ... that relies upon these standards - whether it's Facebook, whether it's Gmail, where it's Skype, whether it's Angry Birds. Suddenly you've been made electronically naked as you go about your activities on the internet.

That decision wasn't debated by any public body, it wasn't authorised by any legislator. In fact, at least in the United States in the 1990s, law enforcement agencies asked specifically for this sort of back door access to internet communications. And our elected representatives in Congress rejected it. They said it was a violation of our civil rights and it was an unnecessary risk to the security of our communications, and so they shut it down.

But what we see is that 10 years later, instead of going back to Congress and asking again, they simply went ahead, and the intelligence community ... said: "We're going to do this. It doesn't matter what Congress says. It doesn't matter what the public thinks. We're going to do this because it provides us an advantage."

And the consequences of that today are unknown because we could have foreign adversaries exploiting those back doors that intelligence agencies in countries like the United Kingdom, intelligence agencies like GCHQ, put into our communications ... and we have no idea that it's occurring.

What last year's revelations showed us was irrefutable evidence that unencrypted communications on the internet are no longer safe and cannot be trusted. Their integrity has been compromised and we need new security pro[grams] to protect them. Any communications that are transmitted over the internet, over any networked line, should be encrypted by default. That's what last year showed us.

Privacy

Of course we can imagine hypotheticals in which some sort of mass surveillance system, facial recognition system, would be effective in preventing crime. In the same way we can imagine hypotheticals in which, if we allowed police to enter our homes freely and search them when we're gone at work, we'd be able to discover elements of crime and drug use and any kind of social ill. But we draw the line, and we have to draw that line somewhere. The question is, why are our private details that are transmitted online, why are our private details that are stored on our personal devices, any different [from] the details and private records of our lives that are stored in our private journals?

There shouldn't be this distinction between digital information and printed information. But governments, in the United States and many other countries around the world, increasingly seek to make that distinction because they recognise that it actively increases their powers of investigation.

Whether technology is compatible with privacy

Absolutely. Technology can actually increase privacy but not if we sleepwalk into new applications of it without considering the implications of these new technologies.

Congress rejected calls for back door access to communication programs in the 1990s. Photograph: Michael Reynolds/EPA

Any new technology when applied at scale, when networked, basically creates a new mesh of sensors in our lives that detect something - they could be changes in the weather, they could be our calling habits, they could be the way we purchase things, they could be the things we like, they could be the temperature we like our bathtubs.

If we don't consider the implications of these new technologies as we develop and apply them, it could be dangerous. But as we increase our level of sophistication about the threats represented by new technologies as they're rolled out, we can balance the capabilities of these technologies with protections that are engineered in them to make sure that these details about ourselves, about our lives, about the way we live, are only seen by those that should truly have access to them.

Most reasonable people would grant that privacy is a function of liberty. And if we get rid of privacy, we're making ourselves less free. If we want to live in open and liberal societies, we need to have safe spaces where we can experiment with new thoughts, new ideas, and [where] we can discover what it is we really think and what we really believe in without being judged. If we can't have the privacy of our bedrooms, if we can't have the privacy of our notes on our computer, if we can't have the privacy of our electronic diaries, we can't have privacy at all.

When he last read Nineteen Eighty-Four

Actually quite some time ago. Contrary to popular belief I don't think we are exactly in the Nineteen Eighty-Four universe. The danger is that we can see how [Orwell's] technologies that are [in] Nineteen Eighty-Four now seem unimaginative and quaint. They talked about things like microphones implanted in bushes and cameras in TVs that look back at us. Nowadays we've got webcams that go with us everywhere. We buy cell phones that are the equivalent of a network microphone that we carry around in our pockets with us voluntarily as we go from place to place and move about our lives.

Nineteen Eighty-Four is an important book but we should not bind ourselves to the limits of the author's imagination. Time has shown that the world is much more unpredictable and dangerous than that.

The politics and oversight of intelligence

That's probably ... the single most important factor that explains the failures [in] oversight that we've seen in almost every western government. Normally the people who are overseeing intelligence agencies are the most senior members of a public body, they're the civil servants who have been around longer than the furniture. And it's because they feel these people can be trusted, they've been here, they've got their heads in the right place.

But we need to think of it in terms of literacy, because technology is a new system of communication, it's a new set of symbols that people have to intuitively understand. It's like something that you learn, … just like how you learn to write letters in school. You've learned to use computers and how they interact, how they communicate. And technical literacy in our society is a rare and precious resource. This is why so many IT consultants who basically just fix printers make very good salaries, because not everybody knows this stuff. And we need this in government, we need advocates, we need specialists, we need experts, [who] work in the service of these senior civil servants and so on, and they can aid and explain and interpret in the same way [as a] foreign language interpreter.

The critical question is, do we want public policies regulating intelligence agencies, or do we want intelligence agencies that determine their own policies, that determine their own regulations, that we have no control or oversight over? And I think that is a critical distinction.

Whether he will give evidence to the UK's intelligence and security committee

I think in general it's appropriate for any legislative body to hear from someone … in person. There are of course circumstances where it's not possible. But if you're talking about actual witness testimonies versus expert testimony, I think it's valuable that you actually make sure that they're in person, on the floor of parliament, so you're not accidentally or incidentally exposing them to unnecessary legal liability.

The incident forcing Bolivian president Evo Morales's plane to land

I was like first off, wow, their intelligence sucks, from listening to everything … But two, are they really going to the point of completely humiliating the president of a Latin American nation, the representative of so many people, the only indigenous president around there? It was just shockingly poorly thought out and yet they did it anyway, and they keep, they kept at these sort of mistakes … I almost felt like I had some friend in government just saying: "Oh yes, do that, absolutely, it's great."

His life in Russia and whether people recognise him

There's actually not that much difference. You know, I think there are guys who are just hoping to see me sad. And they're going to continue to be disappointed. … I don't live in absolute secrecy. I live a pretty open life. But … I don't want to be a celebrity, I don't want to go somewhere and have people pay attention to me, just as I don't want to do that in the media. There are much more important issues in the world than me and what's going on in my life and we should be focusing on those.

What I buy at the grocery store shouldn't really be of interest to anyone. And if I'm recognised, I'm recognised. My daily life in my estimation isn't of interest to anybody.

Bolivia's president Evo Morales, centre, enters his plane after it was rerouted to Austria. Photograph: Hans Punz/AP

I get recognised. It's a little awkward at times because my Russian's not as good as it should be. I'm still learning. But yeah, every now and then somebody does. [He refuses to give a demonstration] The last thing I want is clips of me speaking Russian floating around the internet.

[On being pictured on a Moscow tourist boat] Right, I didn't look happy in that picture. [On pushing a loaded shopping trolley across a road] You know I actually don't know because it was so far away and it was blurry. I mean it could have been me.

[On allegedly going out in disguise] Before I go to the grocery store, I make sure to put on, you know, my Groucho Marx glasses and nose and moustache... No, I don't wander around in disguise.

I'm much happier here in Russia than I would be facing an unfair trial in which I can't even present a public interest defence to a jury of my peers. We've asked [the] government again and again to provide a fair trial and they've declined. And I feel very fortunate to have received asylum. Russia's a modern country and it's been good to me so, yeah, I have a pretty normal life and I would absolutely like to continue to be able to travel as I have in the past. I'd love to be able to visit western Europe again but that's not a decision for me to make, that's for the publics and the governments of each of those independent countries.

Learning Russian and reading Dostoevsky

My Russian and my mastery of Dostoevsky are both less developed than they could be but I enjoy it. Brothers Karamazov, I think that is on the list next. I enjoy learning and it's been a really good experience.

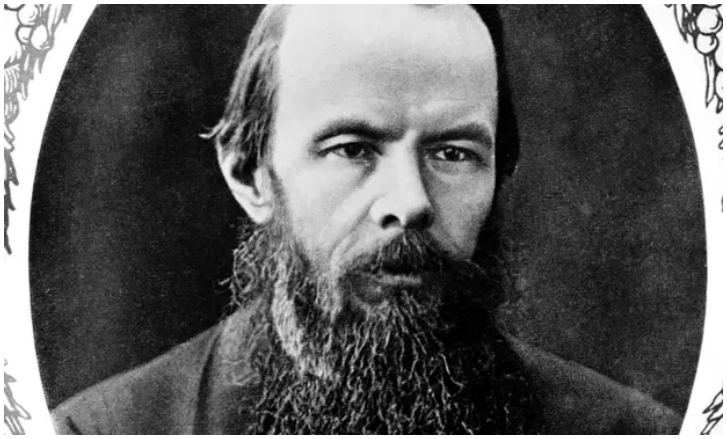
I read a lot of political books nowadays. I try to increase my sophistication to match my environment. Currently, I'm reading a Dan Ellsberg memoir, Secrets, about his release of the Pentagon papers.

Being under surveillance

I don't detect surveillance oppressively, actively, but I think it's reasonable to assume that I am under surveillance. Anyone in my position surely is subject to some surveillance but you take the precautions you can to make sure that even if you are under surveillance, there's no sensitive information for you to expose.

How he spends his time

Recently, I've been spending a lot of time thinking about press freedom issues in addition to the ordinary individual's private communications, and I've been partnering with civil liberties organisations to see where we can contribute and try to create new tools, new techniques, new technologies that will make sure our rights are protected regardless of the status of law in a given jurisdiction.



Snowden revealed he is reading Dostoevsky as he tries to improve his Russian. Photograph: Bettmann/CORBIS

Imagine an app or a cell phone or an operating system for a cell phone or a small device, anything that would allow people to have free and ready access to meaningfully secure communications platforms that don't require sophistication to use and operate.

We may be able to rely on the possibility of reform in the United States, the United Kingdom, some other modern developed democracy. But there are a lot of people in a lot of places who can't rely on that. And so, moving forward, I'm going to be spending more and more time trying to create new tools that guarantee rights to them that may not be available through legal guarantees. Because something that we so often forget in the dialogue about security versus privacy is [that it is] really a misstatement of the issue, which is liberty versus security.

The Boston marathon bombing

Despite the fact that the communications of everybody in America were currently being intercepted, they didn't catch the Boston bombers, despite the fact that the Russian intelligence service specifically warned the FBI that these individuals were known to be associated with Islamic terror groups.

We didn't actually fully investigate them, we just made a cursory visit and went back to all of our keyboards looking at everybody's emails and text messages.

The question of the Boston bombings is not what kind of mass surveillance do we put the whole of society under to prevent every possible perceivable crime that might happen in future, the question is why didn't we follow up when … we were specifically warned about these individuals, and they then later turned out to be a real threat. What we have learned in case studies of terrorism over the last decade … is that almost every terrorist act that is uncovered, almost everyone who's convicted, successfully prosecuted, put in jail, every plot that is disrupted, is not a product of mass surveillance, it's not a product of the kind of indiscriminate surveillance we see today. They're all products of targeted surveillance, traditional surveillance, the kind of boots on the ground, investigate and learn, done by real investigators interviewing real people and following specifically justified leads that occurred as a process of investigation. No single terrorist act, including the Boston bombs, was ever

caught as a result of mass surveillance in the United States. And those numbers are similar around the world as I understand it.

It seems reasonable to expect when we have clear evidence that these programs are ineffective, we should take resources out of ineffective mass surveillance programs and re-allocate them toward the sort of traditional targeted surveillance that's been shown to be effective for hundreds of years.

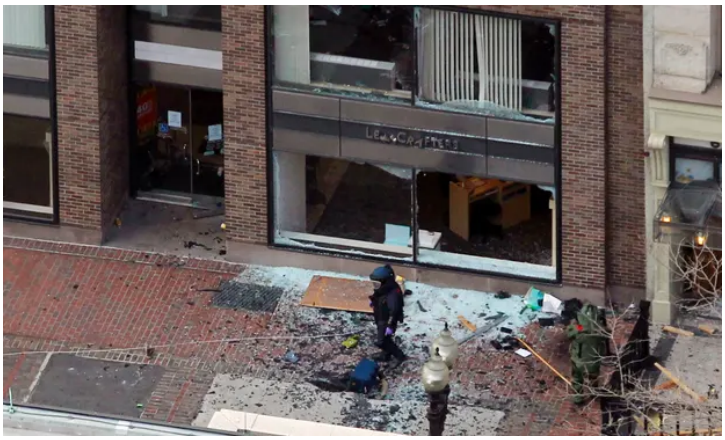
Technology in general

[Does he use dropbox?] They just put Condoleezza Rice on their board, who is probably the most anti-privacy official you can imagine, she's one of the ones who oversaw Stellar Wind and thought it was a great idea. So they're very hostile to privacy. While we may not see immediate revolutionary change, the reality is that technology workers represent an important class that provides an important service to society.

They possess a unique level of technological literacy that allows them to work against our common rights or for them. And what I've seen over the last year is that there is a tremendously strong consensus among technology workers that our private communications should stay private, that we should increase protections against this sort of overreach and abuse by intelligence agencies, and that mass surveillance should not be an issue.

[Why should we trust Google any more than we trust the State?] For one you don't have to. Association with Google is voluntary. But it does raise an important question. And I would say, while there is a distinction in that - Google can't put you in jail, Google can't task a drone to drop a bomb on your house - we shouldn't trust them without verifying what their activities are, how they're using our data.

We should have some kind of civil protection, some kind of civil actions that provide for recourse and the review of companies' use of data. And we need to have at least a broad social agreement about where these lines should be drawn without unnecessarily harming new models of business and new services that we might not be able to anticipate today that we'll need tomorrow. ... I don't use Google. I have used Skype and Google hangouts, which are great but unfortunately security compromised services, for public talks where they've been required but I wouldn't use it for personal communications.



The site of an explosion that went off during the Boston marathon in 2013. Photograph: Jessica Rinaldi/Reuters

I think everybody has some exposure to proprietary software in their lives, even if they're not aware of it. Your cell phones for example are running tons and tons of proprietary code from all the different chip manufacturers and all of the different cell phone providers.

We are moving very slowly but meaningfully in the direction of free and open software that's reviewable, or, even if you can't do it, a community of technologists [who] can look at what these devices are really doing on the software level and say, is this secure, is this appropriate, is there anything malicious or strange in here? That increases the level of security for everybody in our communities.

We don't want to see a fragmentation of the internet. That doesn't serve anybody's interests, whether it's in Brazil, whether it's in Germany or any other country in the world. What we need, we need common protocols that protect data, that protect communications regardless of the jurisdiction through which they transmit.

For example, you wouldn't want a French citizen who sends a network communication that goes to a service in the United States to have that communication monitored or manipulated or reviewed in every country that it transits through. And the same thing in reverse. And if that applies in European countries, that should also apply in Latin American countries, that should apply in Asian countries, that should apply in African countries.

And the only way that's going to happen is by improving the security of our common stand, it's about the way we communicate in general on the internet, the underlying infrastructure across which we all communicate.

Criticisms about the damage he caused

The fact that people know communications can be monitored does not stop people from communicating … because the only choices are to accept the risk of being monitored or to not communicate at all. And when we're talking about things like terrorist cells, nuclear proliferators - these are organised cells. These are things an individual cannot do on their own. So if they abstain from communicating we've already won. If we've basically talked the terrorists out of using our modern communications networks, we have benefited in terms of security - we haven't lost in terms of security.

[On claims he was weakening the democracy he professed trying to protect] What those intelligence officials are arguing is that democracy is unsustainable as a model, that the public can't be entrusted to make those decisions, that we should give up on them and move to an authoritarian system of government. But I think the public, when we look at this independently and make our own decisions, we're not swayed by these overblown claims of harm that are never backed up in the evidence. The question that these intelligence agencies are asking us is, do we want to live in a democracy where we may face some occasional risk from actual harm, which we cannot predict and we cannot protect ourselves from? Or would we rather live under a Chinese model or a Russian model where it's a more controlled society, but it's also less free?

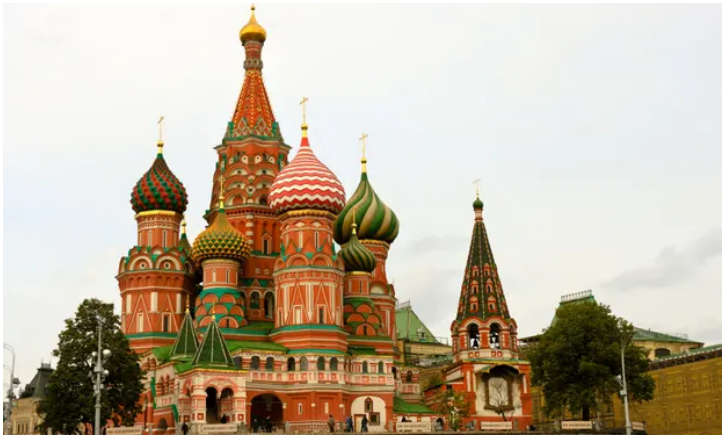
The question is not what government surveillance programmes can the public know about, it's a question of to what detail. We've seen all of these spy chiefs come out and say the atmosphere's going to boil off … the world is going to end, the sky's falling, and yet it hasn't happened in any case at all. So the only people who are rubbing their hands with glee are the reformers who are seeing more and more evidence that the governments overreached here and are incapable of defending claims that they made again and again and again since these publications started.

I can tell you right now that in the wake of the last year there are still terrorists getting hauled up, there are still communications being intercepted. You know there are still successes in intelligence operations that are being carried out all around the world.

Criticisms about hypocrisy and selective outrage

People say you're either naive or have double standards. Every country in the world does this. And that's actually not true. I mean surely not every country in the world even has the resources for an intelligence agency. If we say, okay what about top class intelligence agencies? Are they all doing the same thing? We can see the answer is no.

Somebody has to be first, somebody has to develop the technology, somebody has to apply the technology and that's what we're seeing. We're seeing the United States, and other countries in the five eyes alliance, breaking new ground on how to intrude on the private lives of both legitimate targets and everyone else who's caught up in the dragnet surveillance.



Snowden says the US state department stranded him in Moscow, where he has recently asked to renew his permit to stay.
Photograph: Alamy

Additionally, we know for a fact that some countries do not spy in the same manner that we do. People can claim selective outrage but when we're finding ... CIA spy after CIA spy in Germany week by week but we're not finding any German spies in the United States and the German government claims that it doesn't have those kind of spies you know there's no evidence to make these kind of claims.

Again, if we're going to argue that this is the case we should probably show proof, some sort of evidence, even the tiniest shred, simply an indication that it's occurring before we claim it as fact. It may be that by seizing all of the records for private activities, by watching everywhere we go, by watching everything we do, by monitoring every person we need, by analysing every word we say, by waiting and passing judgment over every association we make and every person we love, that we could uncover a terrorist plot or we could discover more criminals. But is that the kind of society we want to live in? That is the definition of a security state.

Do we want to live in a controlled society or do we want to live in a free society? That's the fundamental question we're being faced with.

Criticisms about his links with Russia

The fact that I didn't bring any classified material with me to Russia means that even if this is a Gulag state, my fingers are being broken every night and I'm being beaten with chains, there's nothing for them to gain. So I think those fears are overblown. What people don't understand about the intelligence community is it's not that we have a finite list of sources and methods, we go on the shelf, we take something off, we use it for spying then we put it back on the shelf. And if that's destroyed it's a permanent hole, we'll never get it back.

[The] intelligence community in the United States and any intelligence agency is much more analogous to a factory that creates ... methods of gathering intelligence. If I happen to know something amazing about an intelligence program and I were beaten or tortured or somehow compromised into giving up this information, it would only be valid for a tiny period. And since the governments that I did work for knew what I had access to, they'd be able to shut those programs down. They would be able to detect a compromise.

The intelligence community knows that I'm not working for any foreign government at all. They anonymously stated to the Washington Post that I'm not an agent of any foreign power, they don't have a warrant out on that basis. And that's because if I were providing information that I know, that's in my head, to some foreign government, the US intelligence community would be able to detect that. They would see changes in the type of information that's going through it. They would see sources go dark that were previously productive. They would see new sources of disinformation appearing in these channels and that hasn't happened.

[It] just looks bad being in Russia. So the first thing to understand is that I never sought to be [in] Russia. I never actively sought out protection here. The state department stranded me in Russia as I was transiting through on my way to Latin America. But I would say, if my reputation is harmed by being here, there or any other place that's okay because it's not about me.

My reputation is not worth anything ... What matters are how people feel about these issues, regardless of your opinion of me. What matters are your rights and how they're being infringed.

New NSA chief Michael Rogers has told Congress he believes Snowden is unlikely to be a Russian spy. Photograph: Lauren Victoria Burke/AP

I've been totally open about the fact that I disapprove of the majority of the recent laws in Russia on internet censorship and surveillance. I think it's entirely inappropriate for any government in any country to insert itself into the regulation of a free press.

We don't want government officials making decisions about we, as a public, what we can and cannot know, what we can and cannot print and how we can and cannot live and I stand by that.

[On Edward Lucas who calls him a "useful idiot"] Yeah. He's crazy. He's not credible at all. ... We've got a new director of the National Security Agency, Michael Rogers, who just came in. He has full access to all classified information. He has full access to the details of the investigation into me.

He has concluded and stated publicly, I believe to both press and to Congress, that I am probably not a Russian spy. There's no evidence for it at all.

If the government had the tiniest indication, the tiniest shred of evidence that, not even that I was working for the Russian government, that I was associating with the Russian government, it would be on the front page of the New York Times by lunch time.

There are always going to be conspiracy theories. People are always going to cast aspersions on people regardless of their activities if they're in a place under a government that's unpopular. I understand that because I myself disapprove of many of the policies of the Russian government. But it's fundamentally irresponsible and journalistically dishonest to accuse someone of working for a foreign government as an agent of foreign power when there's no evidence at all to support it. And I'm not going to respond to every single conspiracy theory that these crackpots online cook up.

Ultimately it just doesn't make sense. If I was a Russian spy I would have flown from Hawaii to Moscow. Why would I have gone to Hong Kong? Why did he go to India [part of Lucas conspiracy theory]? There's a whole thing that I went there unauthorised. It's bullshit, I was on official visits, working at the US embassy. You know, it's not like they didn't know I was there ... and the six-day course afterwards - it wasn't a security course, it was a programming course, but it doesn't matter.

Whether he has read all the documents

I made my own determination broadly about where lines should be drawn, however I felt it was very important that journalists be able to make an independent assessment of what information would be in the public interest to know. And they can't do that unless they have evidence of both programs [that] are justified and evidence of programs [that are] unjustified.

If they only had information about programmes that were clearly criminal it might paint a misleading image of the activities of our intelligence agencies and slant perceptions to make them all the villains that they're not. These are good people trying to do hard work under hard conditions.

Why so many documents

If journalists only report on things that are civil liberties, human rights violating programs, and they don't seem legitimate, justified programs that do help keep us safe, that do help us in our time of war, that do protect critical infrastructure, and again the broad outlines, not every detail, but enough to show that there are good uses and good purposes of these, we would actually be misled by the press as opposed to be served by the press.

I recognised that I can't make that decision about the impressions we should be giving. That should be made by journalists, independently, by their institutions or editors.

The obligation on professionals to change their digital ways

Edward Snowden with Ewen MacAskill, left, and Alan Rusbridger in Moscow. Photograph: Alex Healey

An unfortunate side effect of the development of all these new surveillance technologies is that the work of journalism has become immeasurably harder than it ever has been in the past. Journalists have to be particularly conscious about any sort of network signalling, any sort of connection, any sort of licence plate reading device that they pass on their way to a meeting point, any place they use their credit card, any place they take their phone, any email contact they have with the source because that very first contact, before encrypted communications are established, is enough to give it all away.

No matter how careful you are from that point on, no matter how sophisticated your source, journalists have to be sure that they make no mistakes at all in the very beginning to the very end of a source relationship or they're placing people actively at risk. Lawyers are in the same position. And investigators. And doctors.

It's a constantly increasing list and one that we're not even aware of today. I would say lawyers, doctors, investigators, possibly even accountants. Anyone who has an obligation to protect the privacy interests of their clients is facing a new and challenging world and we need new professional training and new professional standards to make sure that we have mechanisms to ensure that the average member of our society can have a reasonable measure of faith in the skills of all the members of these professions.

If we confess something to our priest inside a church that would be private, but is it any different if we send our pastor a private email confessing a crisis that we have in our life?

His future

I made it very clear that I'd like to return to the United States and if the possibility for a fair trial existed, that would be something that could be pursued.

[On his position as rector of Glasgow University?] I'm actually in talks now to try to create a method for holding rector's surgeries, to be able to talk directly to the students and see what I can do, if anything, to help elevate their concerns and make sure they get fully addressed by the university community. Unfortunately, my personal situation, my security situation, has made it difficult to visit directly, but we're actually trying to find a way so I'm not actually confined to a screen but I can actually travel and speak to people directly.

Whether he stays fit

[I'm] probably three steps from death. I mean I don't eat a whole lot. I keep a weird schedule. I used to be very active but just in the recent period I've had too much work to focus on.

The future of intelligence

I'm overly idealistic, because I'm not sure that political reform is going to be the thing that really protects our rights in the future on the issue of digital communications. I'm not sure there's appetite in government to enshrine those protections. I think technical systems can fill that gap to a large extent, because we can encode our systems and values into the protocols that we use to protect [our] relations.

It's likely to end up in the Supreme Court ... and in Europe. Impending court decisions are, in my estimation, likely to introduce additional pressures on to legislators to pass meaningful reform.

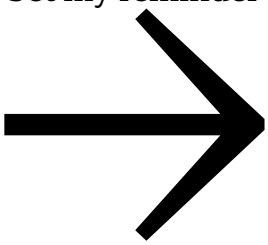
We need to recognise that people have an individual right to privacy but they also have a collective right to privacy. Nobody should have their communications seized and stored for an indefinite period of time without any suspicion or justification, without any suspicion that they're involved in some sort of specific criminality. Just as it would be for any other law enforcement investigation.

Telecommunications providers need to recognise that the interests of their customers come before the interests of any given state. Today, the standard response to any criticism that they face about participation [in] intrusive programs is "we follow the laws of X country when we operate in that country".

Now that may be true, and that may be legally wise, but that doesn't mean they're exempt from advocating for the rights of their customers. When we're trusting them with the most intimate details of our lives, when we're entrusting our private records to their care, they need to make sure that they're a responsible advocate to us as customers, not just legally but socially. And that means they need to use their lobbying abilities, they need to use their commercial clout to force the government to be more responsible in whatever jurisdiction it is, in safeguarding our public interests.

Remind me in September
Email address

Set my reminder



We will use this to send you a single email in September 2020. To find out what personal data we collect and how we use it, please visit our Privacy Policy

We will be in touch to invite you to contribute. Look out for a message in your inbox in September 2020. If you have any questions about contributing, please contact us here.
Topics

- World news
- Internet
- Surveillance
- GCHQ
- Europe
- Russia
- Germany
- interviews