theguardian | TheObserver

The Snowden files: why the British public should be worried about GCHQ

When the Guardian offered John Lanchester access to the GCHQ files, the journalist and novelist was initially unconvinced. But what the papers told him was alarming: that Britain is sliding towards an entirely new kind of surveillance society

John Lanchester

The Guardian, Thursday 3 October 2013 14.01 EDT

In August, the editor of the Guardian rang me up and asked if I would spend a week in New York, reading the GCHQ files whose UK copy the Guardian was forced to destroy. His suggestion was that it might be worthwhile to look at the material not from a perspective of making news but from that of a novelist with an interest in the way we live now.

I took Alan Rusbridger up on his invitation, after an initial reluctance that was based on two main reasons. The first of them was that I don't share the instinctive sense felt by many on the left that it is always wrong for states to have secrets. I'd put it more strongly than that: democratic states need spies.

The philosopher Karl Popper, observing the second world war from his academic post in New Zealand, came up with a great title for his major work of political thought: The Open Society and Its Enemies. It is, in its way, a shocking phrase – why would the open society have enemies? (But then, the title of Charles Repington's The First World War, published in 1920, was shocking too, because it implied that there would be another one.)

We do have enemies, though, enemies who are in deadly earnest; enemies who wish you reading this dead, whoever you are, for no other reason than that you belong to a society like this one. We have enemies who are seeking to break into our governments' computers, with the potential to destroy our infrastructure and, literally, make the lights go out; we have enemies who want to kill as many of us, the more innocent the better, as possible, by any means possible, as a deliberate strategy; we have enemies who want to develop nuclear weapons, and thereby vastly raise the stakes for international diplomacy and the threat of terrorism; and we have common-or-garden serious criminals, who also need watching and catching.

I get all that. It doesn't thrill me to bits that the state has to use the tools of electronic surveillance to keep us safe, but it seems clear to me that it does, and that our right to privacy needs to be qualified, just as our other rights are qualified, in the interest of general security and the common good.

Reassuring read

My week spent reading things that were never meant to be read by outsiders was, from this point of view, largely reassuring. Most of what GCHQ does is exactly the kind of thing we all want it to do. It takes an interest in places such as the Horn of Africa, Iran, and North Korea; it takes an interest in energy security, nuclear proliferation, and in state-sponsored computer hacking.

There doesn't seem to be much in the documents about serious crime, for which GCHQ has a surveillance mandate, but it seems that much of this activity is covered by warrants that belong to other branches of the security apparatus. Most of this surveillance is individually targeted: it concerns specific individuals and specific acts (or intentions to act), and as such, it is not the threat.

Even Julian Assange thinks that, and said as much in his alarming and perceptive book Cypherpunks: "Individual targeting is not the threat." When the state has specific enemies and knows who they are and the kind of harm they intend, it is welcome to target them to make the rest of our polity safe. I say again, on the evidence I've seen, this is mainly what GCHQ does. I would add that the Guardian and its partners have gone to a lot of trouble to prevent any unnecessarily damaging detail about this work being published.

Problems and risks

The problems with GCHQ are to be found in the margins of the material – though they are at the centre of the revelations that have been extracted from the Snowden disclosures, and with good reason. The problem and the risk comes in the area of mass capture of data, or strategic surveillance. This is the kind of intelligence gathering that sucks in data from everyone, everywhere: from phones, internet use from email to website visits, social networking, instant messaging and video calls, and even areas such as video gaming; in short, everything digital.

In the US, the Prism programme may have given the NSA access to the servers of companies such as Google and Facebook; in the UK, GCHQ has gained a similar degree of access via its Tempora programme, and the two of them together have a cable- and network-tapping capabilities collectively called Upstream, which have the ability to intercept anything that travels over the internet. This data is fed into a database called XKeyscore, which allows analysts to extract information "in real time", ie immediately, from a gigantic amount of hoovered-up data.

In addition, the NSA has encouraged technology companies to install secret weaknesses or "backdoors" into their commercially available, supposedly secure products. They have spent a very great deal of money ($250m a year alone on weakening encryption), on breaking commercially available security products. Other revelations have been published in Der Spiegel, and concern the NSA exploitation of technology such as the iPhone.

Access all areas

What this adds up to is a new thing in human history: with a couple of clicks of a mouse, an agent of the state can target your home phone, or your mobile, or your email, or your passport number, or any of your credit card numbers, or your address, or any of your log-ins to a web service.

Using that "selector", the state can get access to all the content of your communications, via any of those channels; can gather information about anyone you communicate with, can get a full picture of all your internet use, can track your location online and offline. It can, in essence, know everything about you, including – thanks to the ability to look at your internet searches – what's on your mind.

To get a rough version of this knowledge, a state once had to bug phones manually, break into houses and intercept letters, and deploy teams of trained watchers to follow your whereabouts. Even then it was a rough and approximate process, vulnerable to all sorts of human error and countermeasures. It can now have something much better than that, a historically unprecedented panoply of surveillance, which it can deploy in a matter of seconds.

This process is not without supervision, of course. In order to target you via one of these "selectors" – that's the technical term – the agent of the state will have to type into a box on his or her computer screen a Miranda number, to show that the process is taking place in response to a specific request for information, and will also need to select a justification under the Human Rights Act. That last isn't too arduous, because the agent can choose the justification from a drop-down menu. This is the way we live now.

British reaction

And yet nobody, at least in Britain, seems to care. In the UK there has been an extraordinary disconnect between the scale and seriousness of what Snowden has revealed, and the scale and seriousness of the response. One of the main reasons for that, I think, is that while some countries are interested in rights, in Britain we are more focused on wrongs.

In Europe and the US, the lines between the citizen and the state are based on an abstract conception of the individual's rights, which is then framed in terms of what the state needs to do.

That's not the case in Britain: although we do have rights, they were arrived at by specific malfeasances and disasters on the part of the state.

Every right that limits the behaviour of the police, from the need for search warrants to the (now heavily qualified) right to silence to habeas corpus itself, comes from the fact that the authorities abused their powers.

This helps to explain why Snowden's revelations, perceived as explosive in American and Europe by both the political right and left, have been greeted here with a weirdly echoing non-response. In the rights-based tradition, the flagrant abuse of individual privacy is self-evidently a bad thing, a (literally) warrantless extension of the power of the state.

Here in the UK, because we've been given no specific instances of specific wrongs having been committed, the story has found it hard to gain traction. Even if there were such instances – just as there were 2,776 rule violations by the NSA last year alone – we wouldn't know anything about them, because the system of judicial inspections at GCHQ is secret.

So it is a perfectly sealed mechanism: we aren't interested in rights in the abstract, and we are prevented by law from hearing about any of the specific abuses which might start to focus our attention.

The documents make clear that GCHQ's eavesdropping abilities are on a scale unmatched anywhere in the free world, and they privately boast about the "more permissive legal environment" in the UK – and yet, nobody seems to care. It's tragicomic that the surveillance story which most gripped the public imagination concerned Poole borough council's use of the Regulation of Investigatory Powers Act 2000 (Ripa) to spy on a family suspected of cheating in regard to school catchment areas.

Helping the bad guys

It's worth taking a moment to ask how helpful the publication of information about this is to the bad guys. (Girls too. But mainly guys.)

The answer is evident, I think, in the under-remarked fact that Osama bin Laden's compound in Abbottabad didn't even have a telephone line running into it. In other words he not only didn't use the net, computers or phones in any way at all, ever, he was suspicious of the actual physical apparatus itself.

This means that the bad guys know very well that they have to be careful. (It should also be noted that the absence of any electronic footprint at the Abbottabad compound was – as depicted in the movie Zero Dark Thirty – a sign to the spies that something fishy was afoot. Nobody innocent has no electronic footprint.)

Some of the jihadi materials I read in the GCHQ documents make it clear that the terrorists are very well aware of these issues. There is a stinging jeer in one jihadi text, apropos a Swedish documentary that made clear certain bugging capabilities in Ericsson's mobile phones: "It is customary in the Scandinavian countries to publish such helpful materials."

While the broad details of general strategic surveillance are shocking and need to be known, the thing that would be helpful to the bad guys is the publication of the specific technical details. These the Guardian and its partners have gone to great lengths to keep secret.

The unkeepable secret

Bear in mind also that these documents were widely circulated: out of the 4.9 million Americans with access to classified information, 480,000 private contractors in the US had the "top-secret" security clearance issued to Snowden.

If hundreds of thousands of people had access to these secrets, how secure were they? The NSA and GCHQ had no idea that Snowden had this material, and apparently still don't know exactly what is in it – which is one reason they've been panicking and freaking out.

But if they didn't know that Snowden had copied it, how could they possibly be sure that someone else hasn't also taken a copy and slipped it to the Chinese or Russians or Iranians or al-Qaida? It was cheeky of Oliver Robbins, deputy national security adviser in the Cabinet Office, to harrumph about "very poor information security practices" on the part of David Miranda, the partner of Guardian journalist Glenn Greenwald who was detained at Heathrow under anti-terror laws.

Our spooks lost at least 58,000 pages of classified documents to a US civilian sitting at a workstation in Hawaii, and did so without realising it had happened. In effect they're saying, "your secrets are safe with us, except when we lose them".

There's one further conclusion to draw from the fact that so many people had access to this material. It means that this story would at some point have come out. A programme of this scale in a modern democracy, involving hundreds of thousands of people with access to the fact of total internet surveillance, was an unkeepable secret. It may be no comfort to Snowden as he faces his future, but someone somewhere would eventually have done what he did. Some dams are fated to burst.

What's new

This brings me to my second reservation about looking at the material: the question of whether it contained anything that we didn't already know. In the Tony Scott movie Enemy of the State, the paranoid former NSA spook played by Gene Hackman lays it out with complete clarity: "The government's been in bed with the entire communications business since the 40s," he says. "They have infected everything. They can get into your bank statement, computer files, email, listen to your phone calls."

That movie came out in 1998, and was a hit, seen by many millions, so even then, in some sense, everybody knew about the work of the NSA/GCHQ. People who kept informed on these subjects have for decades been careful about using specific words over the phone, especially over transatlantic phonelines.

I remember Christopher Hitchens, at the time that concern about Salman Rushdie's welfare was at its peak, wouldn't use his name over the phone but would instead refer to "our mutual friend".

So in some sense, perhaps it's true that everybody knew. This would be analogous to the manner in which we all know surveillance is pervasive in police work, and yet police methods are by law forbidden from being used in evidence, or indeed even mentioned in court. The ban on mentioning police surveillance is there because they don't want us to realise how much of it there is. We all know that, and yet it doesn't seem to matter much. Perhaps the GCHQ stuff was the same?

I've changed my mind about that. It was changing anyway as I thought more about the meaning of Snowden's exposures, and it has changed more still now that I've looked at them first-hand.

Broad definitions

I've said that the concerns over GCHQ are at the margins of what it does: but those margins are very broad. They especially concern things that are referred to in the documents as "SD", which means "sigint development". "Sigint" is signal intelligence, which is what GCHQ does. "Development" means – well, that's the crux of it. It means finding out new things, exploring new technologies, and developing new ways of finding "targets".

When you look at the documents, it appears to be the case that SD provides the legal basis for mass surveillance of the kind revealed in the Tempora and Prism programmes. The mandate of GCHQ – which by the way didn't have a legal basis of any kind until 1994 – is surveillance for reasons of "national security, economic well being, and serious crime".

The main law concerning its activities is Ripa. If you read this 2000 act (which, by the way, I don't recommend, since it's tortured and laborious even by the standards of statute-speak), it's clear that the main focus of its provisions is targeted surveillance. It's about what the spies and cops are allowed to do to catch specific bad guys.

Ripa is pretty broad in its drafting, and it seems apparent that the intention was to let the authorities do anything they wanted with phones and email. And yet, it nowhere explicitly allows the mass interception of communications by people about whom the state has no reason for suspecting anything – which is what programmes such as Tempora and Prism permit.

Behind the times

The law always lags behind technology, that's inevitable. If you look at the first version of the modern Official Secrets Act, which was made law in 1911 and is still the main broad statement of government secrecy in effect today, its first provisions concern the making of "maps and charts".

It is evident that the kind of spying on the lawmakers' minds concerns a chap in plus-fours claiming that he's making drawings of seabirds, only why has he accidentally made accurate sketches of that nearby naval base, and why does he have a heavy German accent … ?

The current spying laws continue to lag behind reality, not only because the spies are less concerned with mysterious birdwatchers, but because life itself has changed.

Formerly, the activities for which the spies were on guard were visible acts of wrongdoing and intelligence-gathering: enemies making maps of naval bases, or breaking into offices, or bribing civil servants, or seducing and blackmailing other spies, or any of the other ways in which they could try to steal secrets.

In the case of modern signals intelligence, this is no longer true. Life has changed. It has changed because of the centrality of computers and digital activity to every aspect of modern living. Digital life is central to work: many of us, perhaps most of us, spend most of our working day using a computer. Digital life is central to our leisure: a huge portion of our discretionary activity has a digital component, even things which look like they are irreducibly un-digital, from cycling to cooking.

(I once happened to visit Google's offices in Victoria, where there's a live stream of people's queries on a huge flat screen. Most of them were in Japanese. My host, who speaks Japanese, glanced at them and looked at her watch. "Recipes," she said. "It's 7pm in Japan, people have just got in from work and are thinking about what to cook.")

As for our relationships and family lives, that has, especially for younger people, become a digital-first activity. Take away Facebook and Twitter, instant messaging and Skype and YouTube, and then – it's hard to imagine, but try – take away the mobile phone, and see the yawning gap where all human interaction used to take place. About the only time we don't use computers is when we're asleep – that's unless we have a gadget that tracks our sleep, or monitors our house temperature, or our burglar alarm, or whatever.

This is the central point about what our spies and security services can now do. They can, for the first time, monitor everything about us, and they can do so with a few clicks of a mouse and – to placate the lawyers – a drop-down menu of justifications.

Surveillance ambitions

Looking at the GCHQ papers, it is clear that there is an ambition to get access to everything digital. That's what engineers do: they seek new capabilities. When it applies to the people who

wish us harm, that's fair enough. Take a hypothetical, but maybe not unthinkable, ability to eavesdrop on any room via an electrical socket. From the GCHQ engineers' point of view, they would do that if they could. And there are a few people out there on whom it would be useful to be able to eavesdrop via an electrical socket. But the price of doing so would be a society that really did have total surveillance. Would it be worth it? Is the risk worth the intrusion?

That example might sound far-fetched, but trust me, it isn't quite as far fetched as all that, and the basic intention on the part of the GCHQ engineers – to get everything – is there.

Consider the direction in which we're moving. Britain has more CCTV cameras than anywhere else in the world, by a huge margin. Nobody knows how many CCTV cameras there are in the country, but the most respectable estimate seems to be the one made by Cheshire police in 2011, which came up with a number of 1.85m. Add to this the capacity for facial recognition software, which already exists and is improving sharply.

Further add the capacity for surveillance brought by the "internet of things", involving the inclusion of internet-enabled computer chips in everything from cars (where they already are, in high-end models) to fridges to plants (which will tweet their minders when they need to be watered). This might sound like science fiction, but the current estimate is that there will be 20bn such devices in use worldwide by 2020.

Add to this the fact that a lot of this electronic potential gives access not just to external real-world data – our locations, our conversations, our contacts books – but to the inside of our heads. I call this the "knowing you're gay" test. Most of us know someone who has plucked up the courage to reveal their homosexuality, only to be cheerfully told by friends and family, "oh, we've known that for years".

Now, though, search engines know facts about people's thoughts and fantasies long before anyone else does. To put it crudely, Google doesn't just know you're gay before you tell your mum; it knows you're gay before you do. And now GCHQ does too.

New society

What this means is that we're moving towards a new kind of society. Britain is already the most spied on, monitored and surveilled democratic society there has ever been. This doesn't seem to have been discussed or debated, and I don't remember ever being asked to vote for it. As for how this trend appears in the GCHQ documents, there is something of a gap between how the spies talk in public and how they can occasionally be found to talk in private.

It is startling to see, for instance, that the justification for the large-scale interception of everybody's internet use seems to be a clause in Ripa allowing interception of "at least one end foreign" communications. Whack on to this a general purpose certificate from the secretary of state, and a general warrant, and bingo, this allows full access to traffic via companies such as Google and Facebook – because their servers are located overseas. I can't believe that that was the intention of the people who drafted Ripa, who were surely thinking more of people taking phone calls from moody bits of Waziristan, rather than your nan searching for cheaper tights.

There is a revealing moment in the most recent piece written for the Guardian by Sir David Omand, former head of GCHQ. He said that "the real debate we should be having … is about what privacy in a cyber-connected world can realistically mean given the volumes of data we

hand over to the private sector in return for our everyday convenience, and the continued need for warranted access for security and law enforcement".

That's a total non-sequitur: Omand seems to think that just because we hand data over to Google and Facebook the government automatically has the right to access it. It's as if, thanks to a global shortage of sticky gum, envelopes can no longer be sealed, so as a result the government awards itself a new right to mass-intercept and read everybody's letters.

Staying within the law

All through the GCHQ material there is a tremendous emphasis on the legal basis of its operations, particularly in respect of article 8 of the Human Rights Act, which grants: "Everyone has the right to respect for his private and family life, his home and his correspondence."

It is repeatedly stated that "GCHQ operates within the law" and that "GCHQ does it legally" and that surveillance always has to be "justified, necessary and proportionate". Good – it would be terrifying if that weren't the case. But if GCHQ seldom breaks the law, it's because the law is so broadly drafted and interpreted it's almost impossible to break.

Also, in the GCHQ papers there are occasional glimpses of a different attitude, usually to be found in slides which are marked as "hidden" in PowerPoint presentations, or in the presenters' notes to other slides. (Many of the clearest documents are internal GCHQ briefings laid out in the form of PowerPoint talks. I was reminded of Malcolm Gladwell's great joke, in response to whether he needed audio-visual aids for a lecture: "All power corrupts, but PowerPoint corrupts absolutely.")

For instance, a legal briefing on the Human Rights Act lists the instances in which it is legal for the state to breach article 8: "In the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."

The notes make the point that national security, public safety and serious crime are the three current reasons for which GCHQ is allowed to eavesdrop, but there is a chilling addition: "'Just' 3 at the moment. No reason why GCHQ's remit would not be changed in the future but this is what we are allowed to do at the moment."

It's usually only in books that people's blood runs cold, but mine did when I read that. "Just" three at the moment: in other words, there are "just" three reasons why GCHQ can violate article 8, the right to privacy. But that could change. It would be legal in human rights terms for GCHQ's mandate to cover "the prevention of disorder", not to mention "the protection of health or morals".

Extending state power

The totalitarian state in Orwell's Nineteen Eighty-Four would need no broader legal justification than that: it really does allow a government to do anything it likes. It was at this point that I became convinced that Snowden's revelations are not just interesting or important but vital, because the state is about to get powers that no state has ever had, and we need to have a public debate about those powers and what their limits are to be.

At a moment of austerity and with a general sense that our state's ability to guarantee prosperity for its citizens is in retreat, that same state is about to make the biggest advance ever in its security powers. In public, the state is shrinking; in private, it is shrinking until it gets just small enough to fit into our phones, our computers, our cars, our fridges, our bedrooms, our thoughts and intentions.

Another secret slide is headed SRA – a mysterious acronym that is not explained. The slide concerns 2P intelligence, 2P meaning second party, ie other countries in the "five eyes" alliance of the US, UK, Canada, Australia and New Zealand. It says that an SRA, whatever it is, "authorises receipt of 2P intelligence on UK based targets where GCHQ has no authorisation".

Since GCHQ can spy on any foreign national it wants, this can only mean the surveillance of people on whom it isn't legal for GCHQ to spy. That looks to me an awful lot like a means of obtaining permission to spy on people – British citizens? – outside the law.

We've heard a lot of talk about the distinction between content and metadata – content being the stuff inside communications, metadata the who and when and where and how of the communication, but not the content. The idea is that the spooks focus on the metadata and ignore the content – so they notice your nan logging on to the net, where and when and for how long, but don't read the actual content of the search.

This distinction is written into the law in both the US and the UK. This would be reassuring, if the notes didn't say this: "GCHQ policy is to treat it pretty much all the same whether it's content or metadata." Put all these together and it is no wonder the documents contain a boast about the UK's "more permissive legal environment".

A new panopticon

The prospect this presents is something like the "panopticon" which Enlightenment philosophers advocated as a design for the ideal prison in the 18th century, and about which the French philosopher Michel Foucault wrote in his book Discipline and Punish. "He who is subjected to a field of visibility, and who knows it, assumes responsibility for the constraints of power; he makes them play spontaneously upon himself; he inscribes in himself the power relations in which he simultaneously plays both roles; he becomes the principle of his own subjection."

When I first read Foucault's account of the panopticon, where the individual at the centre can simultaneously see and judge a whole multitude of other individuals, I thought it was brilliant but overheated. Now, it actually seems like somebody's plan. That's what we risk becoming: a society which is in crucial respects a giant panopticon, where the people with access to our secrets can see, hear, intercept and monitor everything.

Members of the security establishment always want more abilities, more tools, more powers for themselves and fewer rights for us. They never say "thanks a lot, we're good from here, we have everything we need".

Public enemies

From their point of view – the point of view of wanting ever more invasive secret powers – al-Qaida and its affiliates are the perfect enemy. Because al-Qaida combines the characteristics of an ideology and a network, it is everywhere, it is invisible, it is never more dangerous than when you can't see it.

The new emphasis on anticipating the actions of "lone wolf" terrorists raises this danger even higher: the risk of terrorism from people who have never been caught committing a crime, who have no known terrorist affiliations, who are invisible, who could be anywhere … It is the ultimate version of the scare story that used to be called "reds under the bed". How can the state every hope to protect us against people like that, if not by permanent, omnipresent, ever-increasing surveillance?

If we are going to remake society in the image of the fight against terrorism, and put that secret fight at the heart of our democratic order – which is the way we're heading – we need to discuss it, and in public.

Exaggerated risks

When we do so, it might be helpful to consider something called the banana equivalent dose (BED). This is a term used in physics to measure the amount of radiation emitted by a banana. It is a number popular with people who think the dangers of radiation are exaggerated, and who use it to make the point that almost everything is radioactive. A dental x-ray has a BED of 50; serious radiation poisoning takes a BED of 20m; sleeping next to someone for one night has a BED of 0.5 and living within 50 miles of a nuclear power plant for a year has a BED of 0.9.

Since 9/11, 53 people have been killed by terrorists in the UK. Every one of those deaths is tragic. So is every one of the 26,805 deaths to have occurred on Britain's roads between 2002 and 2012 inclusive, an average of 6.67 deaths a day. Let's call that the SDRD, standard daily road deaths. The terrorist toll for 12 years comes to 0.0121 SDRD. This means that 12 years of terrorism has killed as many people in the UK as eight days on our roads.

The security establishment will immediately reply that this figure leaves out deaths of terrorism victims abroad and the lives saved by its secret actions, none of which can be made known without jeopardising current and future operations.

Is that enough of a justification for the scale and extent of what is happening to our privacy? Is the current supervisory regime – which involves senior judges inspecting GCHQ's actions, "within the circle of secrecy", and issuing a secret report – adequate to the scale of the state's powers?

I'd repeat the point that as digital technology, and the ability to enact surveillance through technology, expands its remit, those powers are increasing almost by the day.

In the UK we have a strange sleepy indifference to questions of surveillance and privacy. "The innocent have nothing to fear," says William Hague. But who gets to define who is innocent? Who gets to say what is contradictory to the "economic wellbeing" of the UK? If the innocent have nothing to fear, why is the state reading so many of our emails, and sucking up so much metadata from our phones and computers, under the umbrella of "sigint development"?

Police state

People misunderstand what a police state is. It isn't a country where the police strut around in jackboots; it's a country where the police can do anything they like. Similarly, a security state is one in which the security establishment can do anything it likes.

We are right on the verge of being an entirely new kind of human society, one involving an unprecedented penetration by the state into areas which have always been regarded as private. Do we agree to that? If we don't, this is the last chance to stop it happening. Our rulers will say what all rulers everywhere have always said: that their intentions are good, and we can trust them. They want that to be a sufficient guarantee.

My proposals

There's no need for us to advance any further down this dark road. Here are two specific proposals. The first is that the commissioners who supervise GCHQ include, alongside the senior judges who currently do the work, at least one or two public figures who are publicly known for their advocacy of human rights and government openness. The "circle of secrecy" needs to include some people who are known for not being all that keen on the idea of secrecy.

My second proposal is for a digital bill of rights. The most important proviso on the bill would be that digital surveillance must meet the same degree of explicit targeting as that used in interception of mail and landlines. No more "one end overseas" and "sigint development" loopholes to allow the mass interception of communications. There can be no default assumption that the state is allowed access to our digital life.

As the second most senior judge in the country, Lord Hoffmann, said in 2004 about a previous version of our anti-terrorism laws: "The real threat to the life of the nation, in the sense of a people living in accordance with its traditional laws and political values, comes not from terrorism but from laws like these. That is the true measure of what terrorism may achieve."