Publishing the Snowden Secrets

The Guardian, the government and the people

Gavin Millar QC, Doughty Street Chambers

.....

The whistleblower and the journalists

In late 2012 Edward Snowden was working for Dell at a US military base in Japan. Glenn Greenwald was writing for the Guardian out of Rio, and had a track record of high quality public interest stories about US surveillance and national security issues. A documentary maker in Berlin, Laura Poitras, had a similar CV. Snowden initially contacted them anonymously as a potential NSA whistleblower.

In the three months before May 2013 Snowden was working as a systems administrator for the US government contractor, Booz Allen Hamilton, at an NSA signals intelligence operations centre in Hawaii.

Even in this lowly capacity Snowden had access to substantial quantities of electronic data about NSA surveillance activities – including GCHQ documents on the NSA systems. Snowden initially provided Greenwald with a small sample through a protected means of communication. It was clear to Greenwald from this sample that the US and UK governments were using very broad powers to collect electronic data in a way that went way beyond the targeting suspects.

Greenwald discussed the situation at Guardian editorial level. The upshot was that when Snowden travelled to Hong Kong at the end of May 2013 Greenwald and Ewan MacAskill (an experienced and specialist Guardian national security reporter) went there on behalf of the newspaper to meet him. Laura Poitras also went.

Snowden emphasised to the journalists in Hong Kong that any material he disclosed had to be handled very carefully and that nothing should be done, including by way of publication, which might endanger lives. His stated purpose was that of a whistleblower. He wanted the public to know about the powers being used by USG/HMG over and above those used against targeted individual suspects.

In Greenwald's evidence to the High Court in the Miranda judicial review (about which more later) he said that Snowden

a) did not want the material to fall into the hands of anyone other than professional journalists working to the highest journalistic standards;

b) and only agreed to become a journalistic source on the basis that these journalists would carefully assess the material to determine in each instance that the public interest in the publication outweighed any risk of harm.

The three journalists were with Snowden in Hong Kong for several days. They left with a range of material he had given them, running to thousands of files. They did not each have the same material, however. Snowden provided them with detailed and complex instructions on accessing this heavily encrypted material

The Guardian's work on Snowden, its dealings with the government and its coverage

The coverage itself is well known and the background to it is also now well-documented. The highlights are as follows.

The Guardian's material was analysed by a small group of experienced journalists working in a secure office and under secure systems at the Guardian's premises at Kings Place, near King's Cross. The computers were not networked and were heavily encrypted. There were numerous other protections built in to their working practices.

The first article, on 5 June, reported on an April 2013 order of the secret court established under the US Foreign Intelligence Surveillance Act 1978. It required one of the largest US telecoms providers, Verizon, to give the FBI metadata about all telephone calls on its systems over a 3 month period. The order appeared to have been made under s.1861 of FISA (see slide) at the behest of the Justice Department. This allows orders for the disclosure of *business records* in foreign intelligence/international terrorism investigations. The records were passed by the FBI to the NSA for search. Previously it had not been understood that this sort of metadata would be regarded as a FISA s.1861 *"business record"*.

It had been reported that the Bush administration had been engaged in this sort of data mining but it was not clear whether the Obama administration had been, so the story was of importance. A key point is that details of communications of US citizens/residents were being obtained. It appeared that s.1861 was being used to circumvent the 4th amendment (on screen) requiring a judicial warrant, supported by probable cause, targeted at such persons' communications. There was a political outcry in the US.

On 6 June the Guardian revealed the existence of the NSA's Prism programme by which it obtains access to the servers of the big US corporations which service the internet (Google, Facebook, Apple and so on) in order to collect material for search. They appeared to have been "pragmatic" about the whole exercise (see slide with Eric Schmidt quote).

The material obtained under Prism includes the contents of emails and other communications – as well as user search histories. The Guardian published some slides in a NSA presentation on Prism. These also suggested that data was being collected from the cables running to and from these servers across America.

The USG asserts that it has lawful authority for the Prism collection under s.1881a of FISA 1978 (on screen) which allows the US Attorney and the Director of National Intelligence to authorise:

- the targeting of persons *reasonably believed to be outside of the United States*

- in order to acquire *foreign intelligence information* – a concept broadly defined under FISA so as to include almost any information bearing upon US foreign affairs/relations;

Again communications of US persons are being caught in the data harvesting without a warrant. Issues arise as to whether the *reasonable belief* requirement is being respected in all cases. European politicians and officials express concern that the US is monitoring our citizens in this way (see slide).

At this point our own signals intelligence service, General Communications HQ, comes into the story. The Guardian reveals in a follow-up piece that this Prism data is somehow (it is not clear quite how) being shared by the US Justice Dept with GCHQ. This fact is nowhere to be found in the annual reports of our statutory overseer, the Interception of Communications Commissioner – even though many of those at overseas end, or indeed ends, of the communications passing through the US systems will be in the UK. Thus our legal regime for regulating state interception of these persons' communications, contained in the Regulation of Investigatory Powers Act 2000 ("RIPA"), is apparently being circumvented.

On 10 June the Foreign Secretary refused to confirm or deny in Parliament whether Prism existed (though US authorities have since confirmed its existence) – but claimed, without condescending to detail, that our law was not being circumvented (see slide).

On 9 June 2013 Snowden's identity was published by the Guardian at his request.

On or around 16.6.13 the Guardian provided some of its Snowden material to the US not-for-profit news site, ProPublica. This meant that ProPublica could continue to publish stories if an injunction was obtained against the Guardian in this jurisdiction.

On 17.6.13 the Guardian published its first story solely about GCHQ, revealing how it had intercepted foreign politicians' communications at a G20 summit in London.

On 21.6.13 the Guardian revealed GCHQ's secret operation Tempora**.** Data being carried from telephone exchanges and servers in North America to Europe, on cables running under the Atlantic, is being intercepted on a blanket basis – and searched. This is done under secret agreements with the cable companies licensed by HMG to land the cables in the UK. Most of the material extracted is again content rather than simply metadata (eg recordings of calls or the texts of messages).

It appears that warrants supported by certificates issued by the Foreign Secretary under s.8(4) (on screen) of RIPA provide the ostensible authority for this programme. The Foreign Secretary has ministerial responsibility for the intelligence service (MI6) and GCHQ. I will come back to this point later. This is said to be a joint programme with the NSA and hundreds of analysts of both agencies examine the intercept material. So here the boot would be on the other foot. The US agency can get back from GCHQ the data of US persons passing along these cables without any need to comply with US law.

Before the Tempora article the Guardian's Editor, Alan Rusbridger, had met the Cabinet Secretary (Jeremy Heywood) and the Prime Minister's Director of Communications (Craig Oliver) at Kings Place. They tried to persuade him not to publish the article on the ground that it would jeopardize national security and intelligence work against organised crime. But a decision was nonetheless taken to publish in the public interest. The officials also tried to persuade the Guardian to hand over the ES documents which it held in this country. This request which was politely declined. It was pointed out that Greenwald was working on his

documents out of Rio and his immediate editor was at the Guardian America in New York. The Guardian invited the government to advise it as to its own security arrangements for the material. This invitation was declined.

Perhaps surprisingly the Guardian then heard nothing more from HMG for some 3 weeks. It continued to publish Snowden, though not GCHQ, stories in July.

On 12 July 2012 Jeremy Heywood visited Kings Place again. This time he said that the government might apply for an injunction to prevent further publication of Snowden material. The Guardian then also shared some of its ES material with the New York Times who would be able, like Pro Publica, to publish stories if the Guardian were served with an injunction in this jurisdiction.

Having made the point to the government that the Guardian had access to Snowden documents outside of the jurisdiction, and that others would publish if it could not, the newspaper nonetheless agreed to destroy the hard drives and circuit boards on which the material was located in London. Its staff did this in the presence of two GCHQ operatives in the basement of Kings Place on Saturday 20 July. In a subsequent article Rusbridger memorably described this as *a peculiarly pointless piece of symbolism that understood nothing about the digital age.*

The government then asked who else had the material. Rusbridger told them about the partnership with the New York Times.

In early August the Guardian published articles about the work of GCHQ and, in particular, the generous funding it receives from the NSA for gathering intelligence for the USG. A quoted GCHQ said that it was *less constrained by NSAs concerns about compliance* and that the looseness of the UK regulatory regime for data collection by the state is *an important selling point for Washington.* At this stage Der Spiegel identified some of the cable companies, including BT and Vodaphone, participating in the Tempora operation.

On the morning of 18 August 2013 GG's partner David Miranda was detained under Schedule 7 of the Terrorism Act ("TACT") 2000 (on screen) at Heathrow airport. He was *en route* back to Rio after visiting Laura Poitras in Berlin. The detention by Met Police officers was for the maximum nine hours permitted. Miranda was questioned and journalistic material of Greenwald's that he was taking back to Rio was removed from him. A decision is awaited in a JR challenge to the legality of the detention and seizure (heard earlier this month).

Importantly, HMG had not suggested at any stage in its dealings with the Guardian that by possessing or having access to the Snowden material it, or anyone assisting it in its work, might be involved in terrorism as defined in TACT 2000.

In early September the Guardian co-published an article with the New York Times and Pro Publica in America. This revealed how the NSA and GCHQ, in partnership with internet companies, had managed to insert secret vulnerabilities – known as *backdoors or trapdoors* – into commercial encryption software. To achieve this they had weakened international security standards for the encryption systems. This capacity is particularly important to GCHQ as much of the Tempora intercepted material is encrypted by the time it reaches the UK.

On 4.10.13 the Guardian revealed that the two agencies had targeted the Onion Router ("TOR") network that ensures anonymity for internet traffic in countries where strict state censorship operates (China, Iran, Syria and so on). This was the case despite the fact that this project receives most of its funding from the USG. The agencies were said to want to be able to *de-anonymise* as many TOR users as possible. Their case is encapsulated in one published quote from one of the Snowden documents – *we're interested as bad people use Tor*. The attack is through vulnerable software on an identified TOR user's browser.

At the end of October, after Angela Merkel had accused the US of tapping her mobile, the Guardian revealed that the NSA had routinely monitored the phone conversations of at least 35 world leaders in the past.

The Guardian's approach and position

This can be summarised as follows.

Snowden's decision to blow the whistle meant that the two governments had lost control of the Snowden data before the newspaper became involved. The fact that the information was passed to responsible journalists, however, meant that it was reported responsibly rather than randomly on the internet.

The worldwide political debate stimulated by the Guardian's reporting, in particular about the need for new legislation and oversight arrangements to protect privacy rights against this sort of state surveillance, shows the subject-matter to be of the highest public importance.

The Guardian has shown that very broad surveillance powers have been used for blanket data collection and retention by the state. Truly vast amounts of private information are being collected and retained relating to large numbers of people who are not suspected of any unlawful activity. They, in particular, are entitled to know this.

The newspaper conducted a continuous dialogue with the USG from early June, and our government from mid June, often holding back copy after being persuaded to do so in these discussions. At each stage it has given the state an opportunity to respond to the story under consideration and has included relevant responses in the published copy.

In each case a careful judgment was made at editorial level, taking into account the position/s of the two government/s, that the public interest justified the publication.

Material from only 17 documents out of tens of thousands have been published – less than 1% of the Snowden material.

The Guardian has published the views of numerous experts and run pieces by officials or ex officials making the case against publication. It has fully reported the continuing debate prompted by its reporting, including the voices of those who are critical of the Guardian – and those who call for civil or criminal proceedings to be taken against it.

Whilst the agencies have criticised the Washington Post for inaccurate reporting no such criticisms have been made against the Guardian to date.

Article 8 of the European Convention on Human Rights (on screen)

This is at the heart of the legal concerns in this country about the data harvesting. It guarantees respect for private life, including private information and correspondence. Anyone who may be subject to state measures to gather their private information or communications is the subject of an interference with the A8 right and can complain of a violation of the right.

The interference with their Art 8 rights has to be justified by the government under Art 8(2) as: 1) being *in accordance with law*, 2) pursuing a recognised legitimate aim and 3) *necessary in a democratic society.* In surveillance cases compliance must be ensured through a system of decision-taking and oversight in which the overseer is of an appropriate status to the scale of the intrusion permitted by the decision-taker. This will usually be a judge.

The first requirement (*in accordance with* law) connotes a statutory regime which is detailed, specific and sufficiently clear to enable those whose rights may be interfered with to know where they stand in law.

The Regulation of Investigatory Powers Act

This contains the relevant legal regime in this country. Much has been said about RIPA in the ensuing debate. It was enacted to regulate state

interception and collection/disclosure of communications information long before vast quantities were generated by the internet. It is clearly no longer fit for purpose.

RIPA distinguishes between *internal and external surveillance.* As with the 4th Amendment in the US an *internal* communication (one neither sent nor received outside the British Isles[1]) can only be intercepted under a warrant targeting a particular person or premises[2]. "*Factors*" for identifying (ie limiting) the communications to be intercepted must be set out on the warrant[3]. These might identify for example of communications to/from a particular person, address, phone number etc to/from the person or premises targeted. The security and intelligence services get these warrants from a Secretary of State on the basis that they are considered necessary in pursuit of legitimate aims - protecting national security, preventing/detecting serious crime or safeguarding the economic well-being of the UK.

But for an *external* communication (one sent or received outside the British Isles) none of these protections apply. The relevant Secretary of State simply issues a *certificate* under s.8(4) of RIPA which simply gives *descriptions* of intercepted material *the examination of which* is considered necessary in pursuit of one of these 3 "legitimate" aims. The warrant then authorises the examination of such intercept and associated material.

So the $64m question – if such certificates are being used to authorise the Tempora interceptions – is what descriptions are being entered on the certificates of the material being intercepted for examination?

The RIPA regime for interception of internal, but not external, communications has been upheld as A8 compliant at the ECtHR in Strasbourg. Nor has the Strasbourg court considered whether it is fit for purpose in the context of mass data harvesting.

[1] RIPA s.20
[2] RIPA s.8(1)
[3] RIPA s.8(2)

Since the Guardian's reporting in June legal challenges have been brought under Art 8 to Prism and Tempora by a number of individuals and NGOs whose data may have been harvested.

The ground of challenge to the Prism collection is that for the complainants' private information and communications harvested by the NSA in the US, and then provided to GCHQ, there is simply no legal regime at all for regulating their A8 rights - let alone a sufficiently clear and accessible one to pass muster under A8. This is because RIPA does not apply to this activity.

One challenge to Tempora is that it is not covered by sufficiently clear and accessible law. Put differently the RIPA s.8(4) *certificated warrants* procedure does not indicate sufficiently clearly to those who may be affected that it might allow blanket harvesting of *external communications* from the cables in this country.

Another challenge to Tempora (see on screen for the Privacy International challenge), is that – even if provided for by the black letter law in RIPA – the Tempora harvesting is so vast, routine and indiscriminate as to be disproportionate to any legitimate aim being pursued. Nor is it properly overseen by the judiciary. Therefore it cannot be regarded as a *necessary* interference with privacy in a democratic society.

Some of the challenges have been brought in the Investigatory Powers Tribunal ("IPT"), a secretive procedure under which complaints against the security and intelligence service have to be made. This denies the complainant the right to an oral hearing or to see the case advanced by the intelligence agencies or a fully reasoned decision. If these challenges under the procedure mandated in our domestic law fail then applications will be made to Strasbourg.

Another set of challenges has been taken (by some NGOs) directly to the ECtHR, arguing that the IPT procedure cannot give them an effective remedy and there is no need to seek one there before going to Strasbourg. This may be optimistic. Strasbourg is likely to require them

to exhaust their domestic remedies, by going through the IPT procedure, before applying to the ECtHR.

Has there been sufficient oversight of these processes by elected representatives?

In the US it appears that members of the US Senate Intelligence Committee knew certain things, for example about the three month FISA court orders against telecoms providers. But they could not say so because it was classified information. The Europeans have questioned the legislative oversight there (see slide 20 re Sen Diane Feinstein).

The Intelligence and Security Committee ("ISC") of Parliament was originally given an oversight role by the 1994 Intelligence Services Act. Since 25 June 2013 s.1 of the Justice and Security Act 2013 empowers the ISC to oversee the operations of the three security and intelligence agencies – MI5, MI6 and GCHQ. But the PM has to approve each oversight exercise and the Committee cannot require information to be produced to it by the services. It can and usually does sit in private.

Its members have indicated that they were not told about Prism or Tempora. Nor – according to Chris Huhne - were members of the Cabinet or our National Security Council.

So clearly the answer to this question is no. Our elected representatives have let us down.

Did the Guardian have the right to publish? How might the government have prevented some of the Guardian's coverage if it had applied for an interim injunction in June?

There is no equivalent in this country of the First Amendment right given to the US press by the seminal US Supreme Court decision in *NYT Co v United States* in 1971. This gave the New York Times and Washington Post constitutional protection against prior restraint orders sought by the

Nixon administration, aimed at preventing the publication of top secret information in the "Pentagon papers" leaked by Daniel Ellsberg[4]. Justice Hugo Black memorably wrote: *The word 'security' is a broad, vague generality whose contours should not be invoked to abrogate the fundamental law embodied in the First Amendment. The guarding of military and diplomatic secrets at the expense of informed representative government provides no real security...*

Here secret state information can be protected in an action for breach of confidence. Interim orders can be obtained for delivery up of the information held by the newspaper and to restrain its publication. The latter can be obtained by the state showing that the damage which the publication will do to national security, prevention of crime or foreign relations, for example, will outweigh the benefits of public discussion. All of this was established in the 1980s[5].

Now, however, s.6 of the Human Rights Act 1998 prevents a court from restraining publication if this would be incompatible with the free speech rights of the newspaper under Art 10 of the Convention (on screen).

This gives perhaps a stronger, albeit still qualified, right to publish such material than before. It was this qualified right that the Guardian was exercising when it started publishing the Snowden stories in June.

Just how strong is it? Strasbourg gives strong protection to journalists when acting as the *public's watchdog* over the activities of government – and when publishing responsibly in the public interest. In this situation a compelling case has to be made out on the facts that the protection of

[4] The US SC imposed a *heavy burden* on the executive in such cases to justify prior restraint. Asserting national security interests was regarded as too broad to legitimize prior restraint. The issue is does publication of this material cause a *grave and irreparable danger*?

[5] The common law as it existed before the Human Rights Act 1998 is set out in a decision of the House of Lords in 1998 which considered whether an injunction could be obtained to prevent publication in the UK of a memoir by a former intelligence officer, Peter Wright (the *Spycatcher* case). The book contained government secrets and alleged unlawful intelligence gathering activities by the Security Service. The Judicial Committee held that the government could only get an injunction to prevent publication of state secrets if it could show a particular public interest reason for preventing it. Damage to national security or relations with allies would suffice. The public interest case for restraining publication would then have to be balanced against the public interest in disclosure and discussion of the secret information by the court deciding whether to grant the junction.

the public interest in national security and the like justifies a restraint on press freedom as *necessary in a democratic society*.

Would the government have succeeded in doing this if it had tried, as threatened in July, or earlier in June?

- On the Guardian's side things are relatively clear. The public interest in its coverage of the Snowden material is now manifest. It might of course have been less apparent to a judge if an application had been made right at the start of the saga, but the issues to be covered by then intended articles could have been set out in written evidence. Hopefully, the public interest nature of the issues to be reported upon would have been obvious to the court. Also the fact that the material was available to journalists, not employed by the Guardian, outside the jurisdiction would be a reason for not making interim orders. It could be argued an injunction would be pointless because the global coverage, if perhaps less elegantly than in Guardian, would have continued anyway;

- The difficulty is in assessing what case the government would have advanced on public interest damage. Certainly numerous strong assertions of damage to the public interest have been made by politicians and government officials since publication. In a speech on 8.10.13 the Director-General of the Security Service, Andrew Parker, said that: *It causes enormous damage to make public* what he called the *reach and limits of GCHQ techniques. It is the gift ...*that the terrorists need *to evade us and strike at will.* But of course any <u>legal</u> case would have had to be made out on detailed evidence placed before a judge at a hearing - and by reference to particular categories of Snowden information that might cause damage in identified ways if published. We just do not know what this case would have looked like because it was not pursued and this does not suggest the government had any great confidence in it. Even if it had been we might never have known what the case was, because an application might have been made for a closed material procedure in which the court and the

government's lawyers would have seen some of the latter's evidence, but not the Guardian's lawyers.

Criminal offences under OSA 1989 and TACT

The view has recently been expressed by certain politicians and, indeed, other newspapers that Guardian journalists should now be investigated for offences under the Official Secrets Act 1989 or even s.58 of the Terrorism Act.

These are deeply disturbing suggestions in a western, liberal democracy.

The issue of journalists being prosecuted under the Official Secrets Act has long been a matter of serious public concern and debate. The 1989 Act creates a number of criminal offences of disclosing classified information without lawful authority. These can be committed by government personnel known in the trade as *insiders.* These cover members of the security and intelligence services, Crown Servants (including military personnel and police) and those working for government contractors.

But there are also two offences in the 1989 Act that can be committed by *outsiders,* such as journalists who receive classified material that has been disclosed without authorisation, and then make an unauthorised disclosure of it themselves. For example by publishing it.

One of these, the OSA 1989 s.6 offence (see screen), covers national security material communicated in confidence by the HMG to another state. The suggestion is that this might catch GCHQ material shared with USG and then disclosed by Snowden as an employee of a USG contractor without the authority of the USG.

For the offence to be committed the disclosure by the defendant journalist must, however, be a damaging one as defined by the 1989 Act. An example is one which can be proved to have damaged to the

work of the security and intelligence services. Since this is a criminal case such damage would have to be proved by the Crown beyond reasonable doubt. So any prosecution of Guardian journalists for publishing Snowden material would, as with the postulated civil proceedings, again require close scrutiny in court of the damage said to have been caused to national security by the publication in issue.

It is not difficult to see that the Crown might struggle to persuade a jury of this in circumstances where it had not even tried to obtain an injunction to prevent publication at the time.

There is also a *mens rea* defence under OSA s.6 which is available to the Guardian. This is that it did not have *reasonable cause to believe* that the small amounts of information which it decided it could properly publish in the public interest would be damaging in this way.

Worryingly however, there is still (twenty-four years after its enactment and one Human Rights Act later) no public interest speech defence available to a journalist charged under these *outsider* provisions in the OSA. This makes it likely that that the Art 10 rights of a journalist prosecuted or convicted for publishing material responsibly and in the public interest would be violated. The recent threatening views, very publicly expressed, referred to above only serve to emphasise the pressing need for such a defence. Those expressing them might pause and ask themselves why these two, out of date, *outsider* offences have never once been used against a journalist since 1989.

Yet more recently, and even more worryingly, there have been novel suggestions that the Guardian might be investigated for alleged offences under s.58/58A of TACT. These criminalise:

- possession of information likely to be of use in terrorism;

- eliciting, publishing or communicating such information where it is about military or intelligence personnel.

These suggestions are also bizarre for three reasons.

First, although there is again no public interest journalism defence under these sections, it is a defence to show a reasonable excuse for the acts in issue. Exercising the right of a journalist to investigate and publish responsibly in the public interest is surely such *reasonable excuse.* If it is not I do not know what it is.

Secondly because the Guardian has taken great care not to publish any information about service or intelligence personnel. So the s.58A offence does not arise at all.

Thirdly because in each of these offences there is no harm, or damage, to national security requirement at all. In other words the prosecution can get a conviction without having to prove any actual damage to this public interest. This means, as those making the threats ought to have found out before making them, that any prosecution of a journalist for these offences would contravene established international human rights norms. I have in mind the position both under Art 10 of the Convention and also its counterpart in the Universal Declaration of Human Rights, Art 19. The UN Human Rights Committee has made clear that it is not compatible with Art 19 *to prosecute journalists... for having disseminated...*information of legitimate interest that does not harm national security[6]. I also have in mind the Johannesburg *Principles on National Security, Freedom of Expression and Access to Information*[7] which state that a journalist cannot be punished on national security grounds for a disclosure which does not harm national security or where the public interest outweighs such harm (see Principle 15).

So, the question is - will there now be a major public debate about whether, and if so how, to reform our approach to state surveillance?

Conclusion

[6] General Comment 34
[7] Noted in resolution 1996/53 of the UN Commission on Human Rights

The NYT journalist who oversaw the publication of the Pentagon papers, Max Frankel, now in his 80s, has astutely observed that the publication did not shorten the Vietnam war or even *stir additional public protest*.

And we Brits can be more passive about our privacy than the Americans, except that is when calling for prosecutions of journalists. In a lecture in Cambridge last week Alastair Campbell alighted on this contrast noting that whilst here ...*One or two Tory MPs called on The Guardian to be prosecuted over Snowden...President Obama ...rang colleagues to apologise and called for a debate on the balance between privacy and public interest and disclosure...*

Only time will tell whether we get the serious national debate the Guardian's coverage of Snowden deserves. A Royal Commission on state surveillance of citizens would be justified. But one thing is for sure. We will all think differently about the big US tech companies in the future. Perhaps even more than the governments it is time for them to tell us exactly what they are doing with our private information in the 21st century.