

Craig Murray

Historian, Former Ambassador, Human Rights Activist



Home » Uncategorized » Your Man in the Public Gallery: Assange Hearing Day 14

Your Man in the Public Gallery: Assange Hearing Day 14

September 22, 2020 in Uncategorized by craig

Monday was a frustrating day as the Assange Hearing drifted deep into a fantasy land where nobody knows or is allowed to say that people were tortured in Guantanamo Bay and under extraordinary rendition. The willingness of Judge Baraitser to accept American red lines on what witnesses can and cannot say has combined with a joint and openly stated desire by both judge and prosecution to close this case down quickly by limiting the number of witnesses, the length of their evidence, and the time allowed for closing arguments. For the first time, I am openly critical of the defence legal team who seem to be missing the moment to stop being railroaded and say no, this is wrong, forcing Baraitser to make rulings against them. Instead most of the day was lost to negotiations between prosecution and defence as to what defence evidence could be edited out or omitted.

More of which later.

PROFESSOR CHRISTIAN GROTHOFF

The first witness was Professor Christian Grothoff, a computer scientist based at the University of Berne Institute of Applied Sciences. Prof Grothoff had prepared an analysis of how and when the unredacted cables first came to be released on the internet.

Prof Grothoff was taken through his evidence in chief by Marks Summers QC for the defence. Prof Grothoff testified that Wikileaks had shared the cable cache with David Leigh of the Guardian. This had been done in encrypted form. It had a very strong encryption key; without the long, strong password there would be no way to access it. It was useless without the key. In reply to questions from Summers, Prof Grothoff confirmed that it was standard practice for information to be shared by an online cache with strong encryption. It was standard practice,

and not in any way irresponsible. Banking or medical records might be securely communicated in this way. Once the file is encrypted, it cannot be read without the key, and nor can the key be changed. New copies can of course be made from the unencrypted original with different keys.

Summers then led Prof Grothoff to November 2010 when cables started to be published, initially by partners from the media consortium after redaction. Grothoff said that the next event was a DDOS attack on the Wikileaks site. He explained how a distributed denial of service attack works, hijacking multiple computers to overload the target website with demand. Wikileaks reaction was to encourage people to put up mirrors to maintain the availability of content. He explained this was quite a normal response to a DDOS attack.

Prof Grothoff produced a large list of mirrors created all over the world as a result. Wikileaks had posted instructions on how to set up a mirror. Mirrors set up using these instructions did not contain a copy of the cache of unredacted cables. But at some point, some mirrors started to contain the file with the unredacted cables. These appeared to be few and special sites with mirrors created in other ways than by the Wikileaks instructions. There was some discussion between Grothoff and Summers as to how the cached file may have been hidden in an archive on the Wikileaks site, for example not listed in the directory, and how a created mirror could sweep it up.

Summers then asked Professor Grothoff whether David Leigh released the password. Grothoff replied that yes, Luke Harding and David Leigh had revealed the encryption key in their book on Wikileaks published February 2011. They had used it as a chapter heading, and the text explicitly set out what it was. The copies of the encrypted file on some mirrors were useless until David Leigh posted that key.

Summers So once David Leigh released the encryption key, was it in Wikileaks' power to take down the mirrors?

Grothoff No.

Summers Could they change the encryption key on those copies?

Grothoff No.

Summers Was there anything they could do?

Grothoff Nothing but distract and delay.

Grothoff continued to explain that on 25 August 2011 the magazine Der Freitag had published the story explaining what had happened. It did not itself give out the password or location of the cache, but it made plain to people that it could be done, particularly to those who had already identified either the key or a copy of the file. The next link in the chain of events was that nigelparry.com published a blog article which identified the location of a copy of the

encrypted file. With the key being in David Leigh's book, the material was now effectively out. This resulted within hours in the creation of torrents and then publication of the full archive, unencrypted and unredacted, on Cryptome.org.

Summers asked whether Cryptome was a minor website. Grothoff replied not at all, it was a long established platform for leaked or confidential material and was especially used by journalists.

At this stage Judge Baraitser gave Mark Summers a five minute warning on Prof Grothoff's evidence. He therefore started to speed through events. The next thing that happened, still on 31 August 2011, is that a website MRKVA had made a searchable copy. Torrents also started appearing including on Pirate Bay, a very popular service. On 1 September, according to classified material from the prosecution supplied to Prof Grothoff, the US Government had first accessed the unredacted cache. The document showed this had been via a torrent from Pirate Bay. Wikileaks had made the unredacted cables available on 2 September, after they were already widely available. They had already passed the point where "they could not be stopped".

Neither Pirate Bay nor Cryptome had been prosecuted for the publication. Cryptome is US based.

Joel Smith then rose to cross-examine for the prosecution. He started by addressing the Professor's credentials. He suggested that the Professor was expert in computer analysis, but in putting together a chronology of events he was not expert. Prof Grothoff replied that it had required specialist forensic skills to track the precise chain of events.

Joel Smith then suggested that his chronology of events was dependent on material provided by the defence. Prof Grothoff said that indeed the defence had supplied key evidence, but he had searched extensively for other material and evidence online of the course of events and tested the defence evidence.

Smith then asked Grothoff whether he had withheld any information he should have given as a declaration of interest. Grothoff said he had not, and could not think what Smith was talking about. He had conducted his research fairly and taken great care to test the assertions of the defence against the evidence. Smith then read out an open letter from 2017 to President Trump calling for the prosecution of Assange to be dropped. Grothoff said it was possible, but he had no recollection of having signed it or seeing it. The defence had told him about it on Saturday, but he still did not remember it. The content of the letter seemed reasonable to him, and had a friend asked him to sign then he would probably have done so. But he had no memory of it.

Smith noted that Grothoff was listed as an initial signatory not an online added signatory. Grothoff replied that nevertheless he had no recollection of it. Smith then asked him incredulously "and you cannot remember signing a letter to the President of the United States?" Grothoff again confirmed he could not remember.

Quoting the letter, Smith then asked him "Do you think the prosecution is "a step into the darkness"?". Grothoff replied that he thought it had strong negative ramifications for press freedom worldwide. Lewis then put to Grothoff that he had strong views, and thus was evidently "biased, partial". Grothoff said he was a computer scientist and had been asked to research and give testimony on matters of fact as to what had occurred. He had tested the facts properly and his personal opinions were irrelevant. Smith continued to ask several more questions about the letter and Grothoff's partiality. Altogether Smith asked 14 different questions related to the open letter Grothoff had allegedly signed. He then moved on:

Smith Did you download the cables file yourself during your research?

Grothoff Yes, I did.

Smith Did you download it from the Wikileaks site?

Grothoff No, I believe from Cryptome.

Smith So in summer 2010 David Leigh was given a password and the cache was put up on a public website?

Grothoff No, it was put on a website but not public. It was in a hidden directory.

Smith So how did it end up on mirror sites if not public?

Grothoff It depends how the specific mirror is created. On the Wikileaks site the encrypted cache was not an available field. Different mirroring techniques might sweep up archive files.

Smith Wikileaks had asked for the creation of mirrors?

Grothoff Yes.

Smith The strength of a password is irrelevant if you cannot control the people who have it.

Grothoff That is true. The human is always the weakest link in the system. It is difficult to guard against a bad faith actor, like David Leigh.

Smith How many people did Wikileaks give the key in the summer of 2010?

Grothoff It appears from his book only to David Leigh. He then gave it to the hundreds of thousands who had access to his book.

Smith Is it true that 50 media organisations and NGOs were eventually involved in the process of redaction?

Grothoff Yes, but they were not each given access to the entire cache.

Smith How do you know that?

Grothoff It is in David Leigh's book.

Smith How many people in total had access to the cache from those 50 organisations?

Grothoff Only Mr Leigh was given access to the full set. Only Mr Leigh had the encryption key. Julian Assange had been very reluctant to give him that access.

Smith What is your evidence for that statement?

Grothoff It is in David Leigh's book.

Smith That is not what it says.

Smith then read out two long separate passages from Luke Harding and David Leigh's book, both of which indeed made very plain that Assange had given Leigh access to the full cache only with extreme reluctance, and had been cajoled into it, including by David Leigh asking Assange what would happen if he were bundled off to Guantanamo Bay and nobody else but Assange held the password.

Grothoff That is what I said. Harding and Leigh write that it had been a hard struggle to prise the password out of Assange's hand.

Lewis How do you know that the 250,000 cables were not all available to others?

Grothoff In February 2011 David Leigh published his book. Before that I do not have proof Wikileaks gave the password to nobody else. But if so, they have kept entirely quiet about it.

Smith You say that after the DDOS attack Wikileaks requested people to mirror the site globally. They published instructions on how to do it.

Grothoff Yes, but mirrors created using the Wikileaks instructions did not include the encrypted file. In fact this was helpful. They were trying to build a haystack. The existence of so many mirrors without the unencrypted file made it harder to find.

Smith But in 2010 the password had not been released. Why would Wikileaks want to build a haystack then?

Grothoff The effect was to build a haystack. I agree that was probably not the initial motive. It may have been when this mirror creation continued later.

Smith As of December 2010 what Wikileaks are saying is they wish to proliferate the site as they are under attack?

Grothoff Yes

Joel Smith On 23 August 2011 Wikileaks start a mass release of cables?

Grothoff Yes. This is a release of unclassified cables and also ongoing release of redacted classified cables by media partners.

Smith They were releasing cables by country, and putting out tweets saying which countries they were releasing cables for both then and next? (Smith reads from tweets.)

Grothoff Yes. I have verified that these were unclassified cables by searching through these cables on the classification field.

Smith Were some classified secret?

Grothoff No, they were unclassified. I checked this.

Smith Were some marked "strictly protect"?

Grothoff That is not a classification in the classification field. I did not check for that.

Smith Wikileaks boast that they make the files available in a searchable form.

Grothoff Yes, but their search facility was not very good. Much easier to search them in other

ways.

Smith You said Der Freitag stated that the encrypted file was available on mirrors. The article does not say that.

Grothoff No, but it says that it was widely circulating on the internet. That is done by mirroring. They did not use that word, I agree.

Smith The 29 August Der Spiegel article does not publish the password. Then Wikileaks publishes an article claiming these stories are “substantially incorrect”.

Grothoff It points to the password.

Smith Some cables were published classified “Secret”.

Grothoff These were cables that had been redacted fully by the consortium of media experts.

Smith Why do you call them “experts”?

Grothoff They knew the subject matter and the localities.

Smith Why do you call them “experts”?

Grothoff They were experienced journalists who knew what was and was not safe and right to publish. So experts in journalism. You need to distinguish between three types of cable published at this time: 1) classified and redacted; 2) unclassified; 3) the classified and unredacted cache.

Smith Are you aware that some cables were marked “strictly protect”?

Grothoff That is not a designation of a cable. It is applied to individuals. But it does not indicate that they are in danger, merely that for political reasons they do not want to be known as giving evidence to the US government?

Smith How do you know that?

Grothoff It is in the bundle I was sent, and the evidence of other defence witnesses.

Smith You don't know.

Grothoff I do know the “strictly protect” names you are referring to were in safe countries.

Smith Before 31 August you find no evidence of full publication of the entire cache?

Grothoff Yes.

We then went through an excruciatingly long process of Smith querying the evidence for the timing of every publication prior to Wikileaks own publication, and trying to shift back the latest possible time of publication online of various copies, including Cryptome, MRKVA, Pirate Bay and various other torrents. He managed to establish that, depending which time zone you were in, some of this could be attributed to possibly very early on 1 September rather than 31 August, and that it was not possible to put an exact time within a window of a few hours on Cryptome's unredacted publication early in the morning on 1 September.

[This exercise could cut both ways. The timing of a tweet saying a copy or torrent is up and giving a link, must be sent out after the material is put up, which could be some time before sending the tweet.]

Grothoff concluded that at the end of the day we do not know to the minute timings for every publication, but what we can say for certain is that all of the publications discussed, including Cryptome, were before Wikileaks.

Smith then noted that Parry wrote in his blog "This is a bad day for David Leigh and the Guardian. I ran the password from David Leigh's book in an old W/L file..." but did not give the location of the file. This was at 10pm on 31 August. Within 20 minutes Wikileaks was issuing a press release "statement of the betrayal of Wikileaks passwords by the Guardian" and 80 minutes later an editorial. [I think that Smith here was trying to say Wikileaks had published Parry's breakthrough.] Smith then invited Grothoff to agree that when Wikileaks themselves published the full documents later on 2 September, it was more comprehensible and visible than earlier publications. Grothoff replied it was not more comprehensive, it was the same. It was more visible but by that time the cat was well out of the bag and the unredacted cables were spreading rapidly all over the internet. There was no way to stop them.

Mark Summers then re-examined Grothoff and established that the evidence was that the encryption key for the full cache was given to David Leigh and to nobody else. The storage method was secure – Grothoff pointed out that precisely the same method was used to send around the court bundles in this case. Only David Leigh had revealed the password.

On mirror sites, Grothoff confirmed that the Wikileaks instructions created mirrors without the encrypted cache. All the copies of the encrypted cache he could find on other mirrors, were on sites which plainly were created using other methods, for example other software systems. Summers then got Professor Grothoff to explain the methodology he had used to verify the cables published by Wikileaks before the Leigh crash were all unclassified. Apart from dip sampling, this included a correlation of the number published for each country with the number listed as unclassified for each country in the US government directory. These matched in every case.

Summers then attempted to take Grothoff back over the timeline evidence which Joel Smith had put so much effort into muddying, but was prevented from doing so by Baraitser. She had interrupted Summers four times during his re-examination, on the extraordinary basis that this ground was gone over before; extraordinary because that is the point of a re-examination. Baraitser had permitted Smith to ask fourteen successive questions of Grothoff on the subject of why he had signed an open letter. The double standard was very obvious.

Which brings us to a very crucial point. The next witness, Andy Worthington, was at court and ready to give evidence, but was prevented from doing so. The United States government objected to his evidence, about his work on the Guantanamo Detainee files, being heard because it contained allegations of inmates being tortured at Guantanamo.

Baraitser said her ruling was not going to consider whether torture took place at Guantanamo, or if extraordinary rendition had happened. She did not need to hear evidence on these points. Mark Summers replied that the ECHR had ruled on these as facts, but that it was necessary they be stated by witnesses as appropriate as it went to the Article 10 ECHR defence. Lewis maintained the objection from the US government.

Baraitser said she wanted the prosecution and defence to produce a witness schedule that would get the case finished by the end of next week, including closing statements. She wanted them to agree what evidence could and could not be heard. Where possible she wanted evidence in uncontested statements with the defence just reading out the gist.

She also said that she did not want to hear closing arguments in court, but she would have them in writing and the defence and prosecution could just summarise them briefly orally.

What the defence should have said at this moment is "Madam, the dogs in the street know that people were tortured in Guantanamo Bay. In the real world, it is not a disputed fact. If Mr Lewis's instructions were to deny that the earth is round, would our witnesses have to accommodate that? The truth of these matters plainly goes to the Article 10 Defence, and by pandering to the denial of a notorious and plain fact, this court will be held up to mockery. We will not discuss such ludicrous censorship with Mr Lewis. If you wish to rule that there must be no mention of torture in evidence, then so be it."

The defence did not say any of that, but as instructed entered a process with the prosecution lawyers of agreeing the shortening and editing of evidence, a process which took all day and with which Julian showed plain signs of being uncomfortable. Andy Worthington did not get to give his evidence. The only further evidence heard was the reading of the gist of a statement from Cassandra Fairbanks. I did not hear most of this because, having adjourned to 4.30pm, the court re-adjourned earlier than advertised, while Julian's dad John Shipton, the musician MIA and I were away having a coffee. I commend this account by Kevin Gosztola of Fairbanks' startling evidence. It was read quickly by Edward Fitzgerald in "gist", agreed as an uncontested account, and speaks strongly of the political motivation apparent in this prosecution.

I am very concerned about the obvious collusion of the prosecution and the judge to close this case down. The extraordinary conflation of "time management" and excluding evidence which the US Government does not want heard in public is plainly illegitimate. The continual chivvy and interruption of defence counsel in examination when prosecution counsel are allowed endless repetition amounting to harassment and bullying is illegitimate. Some extraordinarily long prosecution cross-examinations, such as that of Carey Shenkman the lawyer, have every appearance of deliberate time wasting and distraction.

Tuesday's witness is Professor Michael Kopelman, the eminent psychiatrist, and the prosecution have indicated they wish to cross-examine him for an extraordinary four hours, which Baraitser agreed against defence objections. Her obsession with time management is distinctly subjective.

Obviously there is a moral question for me in how much of this medical evidence I publish. The decision will be taken in strict accordance with the views of Julian or, if we cannot ascertain that, his family.

Forgive me for pointing out that my ability to provide this coverage is entirely dependent on your kind voluntary subscriptions which keep this blog going. This post is free for anybody to reproduce or republish, including in translation. You are still very welcome to read without subscribing.

Unlike our adversaries including the Integrity Initiative, the 77th Brigade, Bellingcat, the Atlantic Council and hundreds of other warmongering propaganda operations, this blog has no source of state, corporate or institutional finance whatsoever. It runs entirely on voluntary subscriptions from its readers – many of whom do not necessarily agree with the every article, but welcome the alternative voice, insider information and debate.

Subscriptions to keep this blog going are gratefully received.

Choose subscription amount from dropdown box:

Recurring Donations

2 Pounds : £2.00 GBP – monthly



Subscribe



Paypal address for one-off donations: craigmurray1710@btinternet.com

Alternatively by bank transfer or standing order:

Account name

MURRAY CJ

Account number 3 2 1 5 0 9 6 2