From: Harry Percival [REDACTED]
Sent: 05 March 2014 12:15
Subject: Re: GCHQ, Snowden, etc

Dear Sir Malcolm,

Thank you very much for taking the time to see me today. It was a pleasure to meet you.

I do apologise for having put you rather on the defensive during our conversation, since that wasn't my intention; I assume you've been fielding a lot of confrontational questions on this topic, and I sympathise. I'm more interested in your role, as my MP and as head of the ISC, as a potential reformer of the security services and the legislation that surrounds surveillance.

Onto our misunderstanding, or disagreement, about the words "mass surveillance" then. Let me lay out my position as clearly as I can, and maybe we'll be able to see each other's perspective more clearly.

Using the example of emails and undersea fibreoptic cables, although the specific technology doesn't matter too much --

Supposing you have a list of suspected terrorists, and their email addresses, and you want to be able to intercept emails to or from people on that list, as they pass through your fibreoptic cable, and ignore all others. I think I, and the majority of the population, would probably be comfortable with the idea that GCHQ can tap into that cable, and intercept any emails that are to or from a particular address, and save them for later analysis. Everything else is immediately discarded.

So far, so good, we can imagine a robust system of checks and balances around that, and I wouldn't call that mass surveillance. As a law-abiding citizen, I'm fairly happy that no-one will be reading my emails, because I know I'm unlikely to be on anyone's list of suspicious people, or if I am, then someone will realise it's a mistake, and I will be taken off it (and perhaps, in due time, notified of the mistake).

But supposing you also have some things which we called "selectors" in our conversation, and these selectors aren't about specific people or email addresses, but instead they're aimed at trying to spot any email that looks suspicious -- a discussion of bomb-making equipment, for example. Now, to implement that (and this is where I think we had some sort of misunderstanding over terminology), you need to "read everyone's emails" -- by which I mean, you need a computer to scan through the text of all the emails you've intercepted, read their contents, and check for keywords like "bomb" or "C4" or whatever it might be. And now I think we're onto much more dangerous territory, because now, as a law-abiding citizen, I'm not so sure that no-one will be reading my emails. This email, right now, contains the words "bomb" and "C4" -- does that mean it's now a suspicious email, and it's going to be saved for later analysis by a human being? Remember that I'm writing to you from a gmail address, so the email has crossed the border, been through that undersea cable, so it's potentially one that can be tapped.

And now hundreds of questions come up. What is this list of keywords? Who decides which ones are appropriate and which are not? Obviously the list has to be secret, otherwise it would be easy to evade. But in that case, how do you organise legitimate oversight of that list? Where are the checks and balances to ensure that perfectly innocent emails are not stored longer than necessary? What if one of those emails, which it turns out wasn't about terrorism or anything in the remit of MI6, does contain some information about some other crime -- perhaps I'm conspiring with my wife to avoid a speeding fine. Does the MI6 analyst who read my email, determined I am not a terrorist but possibly breaking the law, now have to report my email to the police?

So I hope you can see how, even though we might disagree on whether that counts as "mass surveillance" or not, you can at least see why I might be substantially more worried about this second category of snooping than the first. In the first, there is a priori grounds for suspicion, which can be surrounded in due process. In the second, there are no a priori grounds.

But then the real problem comes when we actually read about the Tempora programme. What the Snowden leaks seem to be revealing is much, much worse than any of what we've discussed above. From what I can tell:

http://www.theguardian.com/uk/2013/jun/21/how-does-gchq-internet-surveillance-work

It seems GCHQ aren't just filtering emails using "selectors", and immediately discarding everything they deem irrelevant. Instead, they are using "buffers" to systematically store *all* the emails that pass through those interception points, and keeping the content for a matter of days -- three days for the "content", ie the body text of the email, and 30 days for the "metadata", which can then be used for analysis of who's talking to whom.

At least, that's how I read those articles and those allegations. If that's not what's happening, then there should be some sort of public denial and explanation of what the misunderstanding is, and what actually is happening. In the meantime, we have to assume it is happening more or less as Snowden has described it, don't we? What else do we have to go on? If all of the above is legal under current UK laws, which it sounds like it probably is under RIPA (leaving aside the ECHR), and it's technically possible, which I'm reasonably convinced it is, then you can see why people assume it is all true? It's what I'd do if I was a spy!

And that, to me, is unquestionably mass surveillance. It means all my emails are being stored, in full, for 3 days, and in metadata form for a whole month, for the intelligence agencies to run whatever searches they see fit. And that makes me very uncomfortable.

One way of thinking about it all is -- what would it take to implement this sort of surveillance in the "real world"? You'd have to get the post office to make photocopies of everyone's letters, and store them for 3 days, and also to record a big list of what the names and addresses on all the letters are, and what post office they were sent from, and keep that list for 30 days. But since it's not just emails, it's also social networks like facebook, you need to imagine the real-world equivalent of that: every time you go to the pub, the landlord asks you to identify yourself, and they write down your name, and they note down the names of everyone you speak to, so that the "metadata" of your real-world conversations can be analysed for the next 30 days. Presumably that would make you as uncomfortable as it would me... So why is it different when it's a computer doing the snooping rather than a post office worker or a pub landlord?

But more than this, we need some serious, concrete justification for all this. I think that's a major thing that's been missing from the debate so far. Where is the evidence that all this snooping is producing useful results? It's been going for several years now, so surely there must be some sort of example case which the security services can point to and say: look, here is a specific example of a planned terrorist attack, which we found out about thanks to this sort of surveillance programme, and here's why this sort of surveillance, and only this sort of surveillance, could possibly have helped us catch them.

Because otherwise it's all justified using "just in case", and I don't think that's good enough. Because, by reductio ad absurdum, if "just in case" is your excuse, then why stop at 3 days or 30 days? why not keep all the emails, and all the metadata, forever?

These are the sorts of questions I'm hoping you're asking, on my behalf and on the behalf of the public, of the security services in your role as chairman of the ISC.

I think the 6 points suggested by the "Don't spy on us" campaign (Liberty, Privacy International, Open Rights Group, Big brother watch et al) are a really good starting point for thinking about reform:

https://www.dontspyonus.org.uk/

1. No surveillance without suspicion.

2. Transparent laws, not secret laws.

3. Judicial not political authorisation.

4. Effective democratic oversight.

5. The right to redress (by which I understand, the right to be informed, after a reasonable period, when you were placed under surveillance which turned out not to be justified).

6. A secure web for all (ie, to make it illegal for security agencies to work to compromise security protocols like those used to encrypt internet banking transactions, which we all rely on).

In our discussion today, and in this email, we've mostly been talking about point 1, what counts as suspicion. I hope you can see what my concerns are on this front, and you can bear them in mind when you're looking for answers from the security services, in terms of what people like me are likely to find convincing, or not...

I hope the other points will seem less controversial, and finding the right framework for answering them will be more of a matter of degrees...

In any case, thanks again for taking the time to see me, and for reading this follow-up email. Thanks for what I don't doubt is your sincere commitment to your work on the ISC, and I hope that you find all this more of a help than a hindrance.

regards,

Harry Percival.
[REDACTED]