Transcript

People, Power and Politics: How Digitization is Revolutionizing Our World

Heather Brooke

Author, *The Revolution Will Be Digitised*

Chair: Richard Sambrook

Global Vice Chairman/ Chief Content Officer, Edelman

Wednesday 28 September 2011

Richard Sambrook:

Good evening everybody and welcome to Chatham House and this discussion this evening about people, power and politics: how digitisation is revolutionizing our world, with Heather Brooke. My name is Richard Sambrook. I currently am Global Vice Chairman at Edelman, formally the BBC and the Reuters Institute at Oxford and it's going to be my pleasure to chair the discussion tonight.

Heather Brooke is the author of this new book, *The Revolution Will Be Digitised: Dispatches From The Information War*, which takes us inside the information war from the hacker spaces of Boston and Berlin to the UK's journalism hub and Iceland's free speech revolution, from the headquarters of Google and Facebook to Cablegate, the murky world of Julian Assange and Wikileaks, and beyond.

So there's an awful lot of issues that we're going to be discussing there. Heather of course is a visiting professor at City University's Department of Journalism, has written for all the main national newspapers as well as presenting and consulting for Channel 4's Dispatches. Her previous books include *Your Right to Know* and *The Silent State.* And she's won numerous awards including the Judges Award at last year's 2010 Press Awards. And of course she's extremely well-known for leading the freedom of information campaign to reveal MPs' expenses.

I'm delighted, Heather, that you're here this evening. She's not going to make a kind of traditional Chatham House 20 to 30 minute keynote. It's simply going to be a discussion. So I'm going to kick it off and we'll be coming out for questions to all of you fairly shortly.

So Heather, obviously the new book, *The Revolution Will Be Digitised*, really captures the current moment where the digital information revolution is having an enormous impact on all sorts of organisations and institutions and I have the feeling that people are caught in the headlights a little bit. We're in transition between old certainties and a new world that we haven't quite reached. We're in the rapids in between. Is that really what you think you're capturing? Give us some examples of what you think that means.

Heather Brooke:

Yeah, definitely. The time I'm writing about in this book is an investigation that I did in 2010 and it goes all across that year. And I felt – well, I felt and so it transpired – that was an incredibly seminal year in the whole, what I call the

'information war', where through the control of information our society is being radically transformed. The point about digitisation, just to explain what I mean by that, is the way that information is no longer a physical commodity. It doesn't have a mass like it used to. So it used to be that if you wanted to leak a bunch of documents, you physically had to carry away these huge boxes of documents and then you had to physically photocopy them somehow. And they had this physical mass, and it was through that mass that they could be controlled by people in power.

When information is digitised, it loses that mass for the most part. It becomes almost ephemeral, it's like an idea; it's like a thought. And it spreads and it can be shared almost instantaneously. So you can take that, and then you combine it with the internet, which is this web in which everybody is talking to each other and sharing information. And you've got the makings of what I think is a digital revolution, which nobody quite knows how to handle it, what to do with it.

One group I found that was particularly well prepared for this were hackers, actually. And there's a kind of very... I would almost call them establishment hackers, if such a thing exists. This is a group in Berlin called the Chaos Computer Club. And they've been going since the 80s. And I went to their meeting in Berlin last December. I just wanted to read, it's a section from the keynote address that a very well-known hacker entrepreneur – his name is Rop Gonggrijp – this is what he said and I think this really speaks about the time that we're in: 'Most of today's politicians realise that nobody in their ministry or any of their expensive consultants can tell them what is going on anymore. They have a steering wheel in their hands without a clue of what, if anything, it's connected to. Our leaders are reassuring us that the ship will certainly survive the growing storm, but on closer inspection, they are either quietly pocketing the silverware or discreetly making their way to the lifeboats.'

Richard Sambrook:

That's a lovely quote, but is it really that bad? Does nobody have the right criteria or the right approach for managing this transition and these changes?

Heather Brooke:

I always thought that America was on the vanguard of understanding sort of radical free speech, because of the constitution and because of the fact that

it's based on enlightenment values which are very much about civil liberties and old school liberal values. And throughout 2009 and 2010, you had a lot of rhetoric from the American government about internet freedom and in fact I quote this speech that Hilary Clinton gave in January 2010, this internet freedom speech which is… she's talking about how there was a new kind of iron curtain that was going around the world and it was kind of an information curtain where you had some countries that had freedom of information and then you had others where information was not free.

But what was surprising to me is that the American government was all very well when it was telling everyone else how to react to extreme radical transparency, but then it had to cope with Wikileaks and it was on the receiving end of information that it definitely didn't want out in the public domain. And the way the government reacted to that, I thought was definitely not the kind of example I think... well, I would have expected.

Richard Sambrook:

Obviously there are, as you say, the kind of digital evangelists and Julian Assange is now kind of pitched at one end of that. But there are many others who are saying it's about radical transparency and accountability and so on. But equally if you have responsibility for government or even for any kind of big organisation, you can't operate unless some of what you do is confidential, can you? How do you reconcile that? And in your research for the book, where does that net out? What are the sorts of pressures and some of the trends around how organisations are trying to net that out and work out the right position?

Heather Brooke:

Yeah, well in the past, the benefit of the doubt was always given over to secrecy. It was always assumed that the danger was in disclosing information. So if there was ever any doubt, you would keep something secret. Now in this age, that's no longer the default position. I think increasingly we see that secrecy has its own costs that we've previously either been blind to or we weren't informed enough about.

I have a chapter about Iceland, which I think is a really interesting example in the book. And so as most people will probably know in this room, Iceland declared bankruptcy. It had a financial meltdown and when they were picking through the remains of how that happened, what they discovered was

collusion between the finance industry, politics and the media. And the glue that set that collusion in place was secrecy. It was very much like we're seeing with the phone hacking. There was this sort of web of interests and one would think that the media's role was to tell the public about what was happening between politics and finance. But in fact they were embroiled in it themselves. And they had stopped representing the public interest and instead were representing the political and the financial interests.

Richard Sambrook:

And so that whole kind of collusion between media and politics, is an interesting theme this year, really. But what draws them across that line? And what's the reaction when radical transparency or Wikileaks or something comes to bear?

Heather Brooke:

Well part of the reason that Iceland has become so radical, it's become the kind of haven for this radical transparency, is because that was a scandal which people very much associated directly with – secrecy. They saw like a causal relationship between the secrecy and the bankruptcy, the meltdown of their society. And they identified secrecy as the enemy, if you will, and so they then decided the solution had to be full transparency.

It was kind of in that scenario that you had Wikileaks came along and posted on its website a bank loan book, a bank called Kaupthing. And it showed inter-bank loans that the bank was making, and that bank tried to suppress the story in Iceland. On the main news there, they tried to broadcast this story about the bank loaning itself money, and the bank got an injunction. And so the news anchor came on and said, 'Here we are, ready to tell you all the news. Unfortunately, I've just been served with this injunction by Kaupthing Bank. However, if you wanted to know what I was going to tell you about, you could look on this website.' And they put the website on there.

So everybody in Iceland piled onto the internet. They looked at this loan book. They were absolutely outraged. I mean, not just outraged about the inter-bank loans, but the fact that they hadn't been told about it. That that was the foundation on which their banking industry was working. And even more than that, they were outraged because the bank had successfully got an injunction on the media to keep them ignorant of these facts. That really seemed to spark a fire under that population.

So then what happened is they sort of banded together and campaigned. They had quite a lot of protests, and when people in Iceland protest, it's not like people here protesting. They go along into their kitchens and they get out all these pots and pans and they start banging on these pans all around parliament. So they called it the kitchen revolution, and that's what they had. They threw out all of the previous politicians. They had a whole new lot in.

And then they passed this proposal for what was called the Icelandic Modern Media Initiative, which is a holistic raft of laws around freedom of speech and freedom of expression.

Richard Sambrook:

So you can see the case for freedom of speech and freedom of expression, although often it's a question of power rather than freedom of speech. But just before we move on from that point, because I'm sure you'll get questioned about this when we open it up. The other side of that, of course, is there are some things which need to be confidential to protect people's lives. In the case of informants in Afghanistan and so on with the Wikileaks documents... What's your view about that? How do you balance that against the great tide towards openness and transparency?

Heather Brooke:

Well, there was always this tension that I think is now... people are more aware about. But certainly Julian Assange behaves like a hacker and certainly the hackers I've met are very much, they have this very simple idea that if you can only get all the information and throw it on the internet, that's going to change society. Suddenly we're going to have a very fair democracy and it's going to make a better world.

What was interesting, when they had to work with journalists, because if you're a journalist you are used to getting quite a lot of information. But the whole professional training of being a journalist is thinking about – as I talk about in the book – the politics of publishing. And there are two things. One is ethical and one is strategic.

And so I use the Afghan war logs publication as an example, because if that had been published differently, I feel it could have really changed the way the American government had to deal with the Afghan War. And what I mean by that is if one maintained the moral high ground on that disclosure, it would have put a lot of pressure on the American government to answer the

revelations that were revealed in those documents. But unfortunately, because of the way Wikileaks published them, which was in what I would call a kind of irresponsible, well not kind of, in an irresponsible way, it left the names of informants in there. And it instantly gave the Pentagon and the Department of Defence an argument as to why that information shouldn't be in the public domain.

Richard Sambrook:

So if we agree that there are circumstances in which information should be redacted or withheld, who anymore is going to be trusted to make that judgement? Because it's not the government. It's not institutions. It's not the media who are some of the least trusted. It's probably not going to be Wikileaks or a radical hacker. So who is trusted to make that judgement in the public interest? Or is there anything like a public interest criteria anymore?

Heather Brooke:

Well, I come to that right at the end of the book, where I try and sort of think outside of the box and think of political solutions to these intractable problems. The idea I had is that we change the sanctions for withholding information. So rather than there being no penalty for withholding information that doesn't cause any harm or they're withholding it because it's embarrassing or they're withholding it to keep power, there should be some kind of sanction for doing that.

And in the same way that in freedom of information around the world, the onus is always… the balance is always on disclosure and the state has to argue why it keeps things secret. But the problem always is in enforcement and who enforces it. And it becomes particularly problematic in the intelligence agencies. Because there you've got this argument of national security and what is happening is that national security is becoming the new word of God, where you can't challenge it. You can't challenge the facts behind why we go to war or why have we put people in prison or why have we occupied a country. And that's where I do kind of think that we need to push the line further.

Richard Sambrook:

Okay, that takes us to the other side of the argument because on the one hand you have a lot of digital evangelists pushing for transparency, openness

and so on. But of course, as a number of people have pointed out, digital technology can also be used by repressive regimes and could be used for all sorts of nefarious purposes as well. So the revolution will be digitised, but it could be all sorts of different revolutions, couldn't it?

Heather Brooke:

And this is the thing about this time of free speech that we have at the moment. It makes a lot of people feel uncomfortable. We've got good things, we have bad things. I mean I think it's really interesting the fact that suddenly in Saudi Arabia, women have the vote. And I really feel that in some way that is a result of what's happening not just in the Middle East uprisings, but the fact that there was this campaign on Twitter where women in Saudi Arabia said, 'We're going to go drive,' because they're not allowed to drive in Saudi Arabia. But they all, they posted videos of themselves driving. And as one woman saw another woman doing it, she thought, well I'm going to do that too. And so suddenly a group of women started driving around Saudi Arabia.

And it's pushing the envelope there. So it gives people power who didn't have power. Equally...

Richard Sambrook:

It can give more power to those who've got it though, as well.

Heather Brooke:

Yeah, and I think this is the danger, is that if we all start putting our lives online, it can empower us as long as we know who has control of that information. And what I investigated in the book a little bit was who does own that information? Who does control it? When we upload all this information onto Facebook, onto Google, onto Apple, where does it go? Who is it shared with? Are they linking it with other databases? Are they running algorithms to predict future terrorists? And in fact, lots of that stuff *is* happening.

Richard Sambrook:

You mentioned something about the, was it the Wire Tappers' Ball?

Heather Brooke:

Yeah, yeah. There's this really interesting conference that they have in Washington DC and it's colloquially known as the Wire Tappers' Ball. And it's all the sort of surveillance industry aficionados go there, and telecoms companies. And somebody I know went. He was a PhD student at the time and he made a surreptitious recording... he surveyed the surveyors at their conference.

And one of the interesting things he taped was an executive from Spring, which is a big telecom [company] in America. And he gave this keynote speech in 2009, in which he... I won't say admitted, but I'll just read what he said. He's talking about the requests they get from law enforcement to intercept and tap telephones:

'My major concern is the volume of requests. We have a lot of things that are automated, but that's just scratching the surface. One of the things, like with our GPS tool, we turned it on the web interface for law enforcement about one year ago last month. And we just passed eight million requests. So there's no way on Earth my team could have handled eight million requests from law enforcement just for GPS alone. So the tool has just really caught on fire with law enforcement. They also love that it's extremely inexpensive to operate, and easy. I just don't know how we'll handle the millions and millions of requests that are going to come in.'

I'm pretty certain that most Spring customers, as most T-Mobile customers, as most O2 customers, have no idea of the level in which their communications can be accessed by the state.

Richard Sambrook:

Presumably we don't need to worry about that unless we're misbehaving?

Heather Brooke:

Well, I want to put paid to this idea that if you've nothing to fear, you've nothing to hide. I interviewed a really interesting guy in this book. He ran the data campaign for the Obama election, when Obama was being elected. And what they do is they just harvest huge troves of databases. And they're doing it for the basis of trying to predict who might vote for Obama in the election.

And he just took me through this whole data business – data brokerage, data dealing. And he showed me this 10,000... well, it was a 464 page dictionary, a

data dictionary, with 10,000 data units in it. So that's for every person, it's 10,000 things that you could find out about that person. Their political association, if they drink Coke or Diet Coke, what sort of magazines do they subscribe to, have they ever had any court cases against them. It's just like a raft of stuff.

The problem is, is how these things are used. It's fine if somebody wants to sell you some products, but increasingly states are accessing all this information. And they're building algorithms to try and predict criminals.

Richard Sambrook:

Have you got examples or illustrations of how it's been used by states in that way?

Heather Brooke:

Well, it's very opaque how it's being used. It's pretty well-known that the National Security Agency in America is building algorithms and it's taking all of these datasets and basically trying to predict who is going to be a problem for us in future. And to me that just seems an incredibly dangerous road for us to go down, that you're no longer innocent until proven guilty. We're starting to imagine or predict who is going to be a problem.

Richard Sambrook:

Just before I open it up, go back to your campaign for MPs' expenses, the freedom of information campaign. Because you talk a little bit about that certainly in the introduction there, and you posit it… I mean the subtitle here is 'Dispatches from the information war'. And the way you describe that campaign, if you like, was an assault on a kind of fusty bewigged establishment that had no idea of how the ground was shifting under its feet. And that seems to be the kind of perspective you bring to a lot of the issues that the digital revolution is throwing up. Talk to us a little bit about what you encountered, and reflecting back now on what happened over MPs' expenses and what's changed since.

Heather Brooke:

Well I got the idea for this book from MPs' expenses, because that was something which just didn't… I never imagined it would be such a big story or

such a big scandal. And really the reason it was such a big story wasn't so much the duck pond or whatever, it was the secrecy. It was the sustained obstruction and secrecy and the sense of arrogance that these people in power thought they could claim money from the taxpayer for public duties and not account for it. And for five years they tried to keep this ideology in place, that because they were our leaders, they didn't have to account to the people for what they did.

It was sort of that, I mean that was definitely what motivated me to go after them. But when it came out, it was never… the whole way through, there was never an acknowledgement by Parliament that the citizen was an equal in power. It was always, everything was dragged out of them. It was a battle. And finally when I won the High Court case, they had no wiggle room, they had to release that information.

And then even then, they were scanning in all the documents. I started to hear rumours that they were trying to redact huge parts of those expense claims. And then they did this incredible thing, which is they tried to… they sort of cooked up this plan between the Conservatives and the Labour Party to push through an amendment… I think they were going to do it through an amendment or a statutory regulation. They were going to try and amend the Freedom of Information Law so that it retrospectively didn't apply to them.

I mean, I just thought it was amazing. The press got wind of it; it became quite a big story. And they were embarrassed and they dropped it. But it was during that time that somebody inside Parliament, must have just been so fed up, outraged, I don't know, that they decided to… they had access to all of that information, and this is the revolutionary thing about digitisation. Initially it had been just all kinds of boxes and pieces of paper and stuff, which nobody could make sense of.

But because it had all been scanned in, it was now a digital archive. And so within an instant, somebody could copy that entire hard drive. It's very tiny. You can take it out, you can sell it to somebody else. You can publish it. And then once that data was out in public, it was incredibly hard for Parliament to say. They tried to contain that story. They tried to keep the power structure the same, but there was such intense pressure from outside.

Richard Sambrook:

So really, just to round that off, the kind of core of… all the examples that you use in your book and in your work has been that digital technology is a tool

which is dramatically shifting power relationships in society – in the UK over MPs' expenses, we could talk about the Arab Spring and all sorts of things. But the role of digital isn't necessarily just because of that, but it's a tool which gets used to shift power relationships.

Heather Brooke:

Yeah. I mean, technology is not the revolutionary thing. It's providing the tool for us to finally implement an idea that we've had for a long time which is a kind of global interconnected democracy. And that's definitely, we could go that way. I think there is a real fight back from traditional power. And by that I mean more authoritarian types of power – the military, the police, the intelligence agencies, government – to try and keep things exactly as they are, not to change. There's a real fear of the public being able to communicate and to connect.

And that's what I think we saw after the riots, where the instant reaction of some politicians was, 'Oh my God, we've got to somehow monitor Twitter. Twitter is dangerous, social networking is dangerous. We have to control it.' And not trusting that people can actually self-regulate. In fact, that's increasingly what we see happening on the internet, is that somebody will… Because the communication is amoral, you can do good things on it, you can do bad things on it.

Somebody might do something bad on the internet. The way to deal with that? There's two ways. One, you can try and use that as an excuse to shut down the internet or control it. Or, you can let the other people on the internet self-regulate. Increasingly, that's what's happened. You see somebody acting outrageously on the internet and everybody piles in and it starts to self-regulate.

Richard Sambrook:

There's a lot I could say about that, but I'm going to leave it to the audience. We've got 30 minutes for questions. If you have one, ideally stand up, wait for the microphone and tell us who you are before you ask a question.