Transcript

The Online Underworld

Jamie Bartlett

Director, Centre for the Analysis of Social Media, Demos; Author, *The Dark Net*

David Anderson QC

Brick Court Chambers and the Government's Independent Reviewer of Terrorism Legislation

Chair: Geoff White

Technology Producer, Channel 4 News

11 September 2014

10 St James's Square, London SW1Y 4LE T +44 (0)20 7957 5700 F +44 (0)20 7957 5710
www.chathamhouse.org
Patron: Her Majesty The Queen Chairman: Stuart Popham QC Director: Dr Robin Niblett Charity Registration Number: 208223

Geoff White

Welcome, everybody, to Chatham House. We've got a couple of announcements to make but I'll introduce the speakers first. Firstly, thank you all for popping along. My name is Geoff White, I'm the technology reporter for Channel 4 News.

My first job in technology was for an internet advertising company, and that was about 1998-99 – about 1998, I think. What was interesting about the web in those days, that I have trouble explaining to people these days, is that it was quite a small place. It was quite a manageable place. If you came across a website that was funny or crazy or outrageous, generally other people in the industry knew about it and you could talk to them about it at the free drinks parties, which in those days happened five to six times a week. I miss those days, I do miss those days. What was interesting for me discovering the 'dark web' some years ago, as some people call it – the dark web, onion sites, however you want to term it. I've got in trouble on Twitter for calling it the dark web. I've tried to use the journalistic shorthand defence, which obviously on Twitter doesn't go very well.

But what interested me about the dark web is it seemed to be a return to those days. It seemed to be a return to a more manageable environment on the web. It seemed to be an act of discovery. It seemed as though if you clicked enough, you could look at genuinely all the pages on there. I think that's part of the appeal of the dark web for people.

But also part of the appeal obviously is it's a hidden area of the web, and that I think is part of the buzz. What's interesting about the dark web and the more fringe areas of the web, and what makes Jamie's book such an interesting read, is that it attracts the sort of darker elements of human behaviour. So Jamie's book, just to be clear, goes beyond the dark web, the onion sites, and looks at the darker recesses of the internet, if you like. Communities have coalesced around those areas that are looking at drug use, they're looking at extreme sex practices, extreme politics – all interesting areas for a book, as you can imagine.

What I'm interested in and what's touched on in the book, but I'd like to hear a bit more about tonight for me, is to what extent does the internet just reflect human behaviour and reflect human personalities – to what extent does the internet actually foster those behaviours? So is the internet simply an actor in the human drama or is it in some way directing us, and directing us to darker areas of our psyche?

Inevitably, of course, that then butts up against issues of legislation, issues of enforcement, issues of freedom of speech and issues of ethics. That's why it's fantastic to have David Anderson QC here, who is not only a very experienced barrister but is also the government's independent reviewer of terrorism legislation, whom I'm sure will have some views on that.

So the stage is set for a fantastic discussion. Just to let you know, there is a drinks reception afterwards, at which point you can all mingle and discuss your views. But for the moment, I'll hand over to the author of *The Dark Net*, Jamie Bartlett.

Jamie Bartlett

Thanks so much. Thanks, everybody, for coming. I'm really delighted to be here and to speak to you about this. Let me say something very quickly about the reason I wrote the book, and then I'm just going to tell you a couple of stories.

We hear, especially over the last couple of years, we constantly hear about these little communities and subcultures that emerge online and pop up into the media. Maybe it's about drugs cultures, child pornography, far-right extremist groups. Then they disappear again and we move on and we think about something else. We worry about something else.

What I always noticed about these stories was very rarely would anybody go into any great detail to try to understand – what are the motivations of people that spend so much of their time in these darker corners of the net? Who are they? What do they get from it? How does being online all the time affect their behaviour, their morality, their sense of themselves, their identity?

So I set myself this challenge and over the course of a year I sort of immersed myself in these cultures. I became a moderator of a trolling group, a secret trolling group. Spent a lot of time up and down the country in pubs with neo-Nazis who spent their entire lives online pushing out their white pride propaganda. I went to – I'm sorry to have to tell you this – to a live webcam sex show, when I did actually get pulled into the show as well. You have to read the book to find out why that happened and what happened as a result of that.

I went in there to try to meet the people that are part of it and as a result – not to be polemic about what people do behind a screen with freedom and perceived anonymity (real or perceived anonymity) but just to present a series of portraits of these darker recesses. Then the people decide what they think about it. So that was the idea of the book.

For tonight's event we're interested in what this means for crime and for law and order and for security. So I'm going to start off with a story about the Silk Road drugs market, which is actually just an online, anonymous marketplace. Has anybody ever been onto this online market? No one ever says so.

Geoff White

I'll say yes, because it's not a crime to have been there.

Jamie Bartlett

It's not a crime to have gone onto the site. It's a crime to do what I did, which was to buy some marijuana from the site, which I documented in the book. The thing about when you go onto the Silk Road, you require this anonymous browser, Tor. The site is hosted as a Tor hidden service, which means it's incredibly hard to locate. It's incredibly hard to find where the website is actually hosted and it's very hard to locate the location of the people that are on there using it. But here's the trick.

So when you go onto the Silk Road, the first thing that strikes you is the unbelievable choice of drugs on offer. You can choose from between 800 or so vendors selling thousands of different varieties of drugs. This creates the sort of dynamic that you will find in any genuine marketplace: competition and choice. Competition and choice means that the vendors are desperate to keep the buyers satisfied. So for example, when I emailed one of the prospective vendors, saying: hello, my name is (I made a name up, of course), I'm new to this website. I would like to buy a tiny amount of marijuana. What do you recommend? A couple of hours later: Dear Sir, thank you so much for your inquiry. I will completely agree – you're new, you should start small. That's an excellent idea, I would do the same. May I recommend this particular type of marijuana, it has excellent reviews from other users. I do hope we can do business together. Best wishes, Drugs Heaven.

As a result, everything on this – people think that this site works because of encryption and you have to pay using bitcoin, the crypto-currency. But that's not why it works. It works because it's introduced a functioning marketplace in an industry where there has not been a marketplace before, not a genuine one. The drugs world is of course characterized by monopolies and cartels, and as a result you cannot predict the purity of the drugs you buy. You have no real recourse. What happens is, sadly, people die unnecessarily from overdosing, when they have heroin laced with anthrax, they don't know the purity of the things that they're putting in their body. They go onto street corners and get themselves beaten up and robbed. Here, it's like buying something on Amazon.

I tell you this story not to encourage any of you to do this. I tell you this because it's part of a story about how crime is changing, and how with very clever traditional methods of introducing a marketplace – stolen really from Amazon and eBay – with the combination of smart encryption technology, it's transforming the way that people can break the law. It makes it far easier.

Actually, this is one of the messages of the whole book: moral ambiguity. I went in there assuming that I knew that this was going to be terrible, but actually there are some potentially quite important plus sides to something like this. It may be extremely confused – something that I saw throughout, in pretty much every subculture I visited.

The other part about the Silk Road, and this is part of the story of how crime is changing, is how incredibly creative and resilient it is. At the end of October, beginning of November, the FBI busted the original Silk Road website. Had been going for about three years. They busted it, they took it down. The Silk Road was gone. You couldn't access it on Tor, you couldn't access it anywhere. Now at the time, there was about three or four similar sites operating in the same way as the Silk Road. Nowhere near as big. They were online and people were using them. Six months later, after that original bust, there are now approximately between 25 and 30 of these sites that operate as a Tor hidden service on the dark net, selling many more drugs than ever before to many more people than ever before. They're smarter. They've learnt from the bust. Their encryption systems are better. They've developed and introduced new systems of payment that offer more security for the buyer. They've even introduced a search engine like Google to be able to choose between different types of sites and different types of drugs. They have learnt from being taken down and now they're bigger than ever.

One of the reasons they're bigger than ever, and it makes you wonder about the power of censorship to stop these things, is because it's not just drugs users that are keeping these sites going. They are supported by this strange ecology of computer programmers, crypto-anarchists, who believe in the idea of an uncensored marketplace where no government can set foot, where no government can control what is bought and sold, where no government can monitor or tax what is happening there. They believe in this for philosophical reasons. It's a political project. The Silk Road is not just about drugs, it's about creating a decentralized, uncensorable marketplace beyond the writ of the government.

So there are those people that are constantly working out ways to undermine the ability of the state to monitor and to censor what people do online. Since Edward Snowden this has grown incredibly quickly. So following the Snowden revelations, and I think this is going to be an extremely important trend over the next couple of years – I've been seeing a huge growth in sort of citizen-led, crowd-source-funded systems of encryption. There are going to be sort of default email systems to allow you to communicate with other people in such a way that it's incredibly hard for a third party to be able to listen in and hear what it is that you're saying or read what it is that you're saying.

These pieces of software are often all open-source and are going to be widely available, and I predict that their usage is going to increase. Indeed, a huge number of people use Tor, the Tor browser, now. Many more people than 12 months ago now use pretty good encryption software as well. It's for very good reasons. There are very good reasons, of course, that people are going to want to keep their communications secret. It's not only in this country that people rely on this software to sell drugs, it's people in Syria that rely on this software to keep them alive. The problem is that exact same technology is always picked up early by the people that have the most to hide, and that is both journalists and drug dealers.

My second point, and this is another thing that I think is covered throughout the book, is the ease with which one can commit quite serious acts of crime and immorality. A very distressing chapter, of course, on child pornography – the availability of child pornography now is absolutely remarkable. It's not that difficult to find, is the great tragedy. Every time that it's closed down, shut down, there are people that have the images saved on their own computers and then re-upload them to new servers, to new websites. It's over the last ten years. Because digital files are just endlessly copyable and shareable at no cost, those images have just spread across the net.

As a result, because it's so easy to find, more and more people – such is humanity, I suppose – more and more people find it. More and more people look for it, knowing that it's there. I interviewed one individual who I believe has recently been convicted of the possession of 3,000 indecent images of children. I don't think, without the ease of how he accessed that material, he would have ever – 20 years ago, he never would have ended up in the place that he did.

I think a similar lesson holds true for things like internet trolling, the sort of low-level criminality of bullying and nastiness online, of stalking online. I did a lot of work on that in the book as well. Incredible number of people, as I'm sure all of you are well aware, incredibly mean and nasty to each other, sharing each other's photos without their permission and bullying and doxing, it's called, sharing people's personal information – simply from the comfort of their own home. That's because it's so much easier to do it.

The relationship between demand and supply and the extent to which it reflects us and our morality, or it exaggerates it, is one of the questions that I try to answer. To be honest with you, I come out of the book not being entirely sure what I think. Certainly magnifies, gives licence to, makes easier some of the darker sides – and some of the lighter sides – of our personality.

I think as a result of some of this, what you're seeing is how the police, in my view, are sort of overwhelmed by the amount of illegal material that's online, overwhelmed by the number of complaints they are receiving about internet bullying, overwhelmed by the number of videos they're being asked to investigate. I'm not entirely sure what the answer is to all of these questions. That's one of the reasons we're here and I'm sure David will have all the answers to this.

But behind it all and underneath it all, at the end when I sort of peeled away all the technology, this was a book about humans, about individuals, about individual morality. Even though I went into the book thinking that it was all going to be quite black and white and I wanted to look at the darker side of internet subcultures, and I was ready to condemn everything, I was ready to be outraged and I was ready to write that outrage, I came away being rather more confused. Rather more moral ambiguity to all of these subjects that I thought initially I'd be convinced about one way or the other, and that's because the closer you look at these problems, the more you find humanity there, and the more you find humanity and all its complexity and all the problems that we bring.

As a result, probably the harder question is not just about the law and what we can do in terms of security and keeping us safe and making sure people are arrested, but what it means for us as a society and our sort of moral compass and our collective idea about what's right and wrong. I think maybe that in a world where everything is accessible and everything can be found and everyone can be communicated with, I think it's that about what it's doing to us and society, rather than how the law keeps up with it, is going to be the more defining question of our time.

Geoff White

Great stuff. Just before I introduce David Anderson, I'll just give you a second to log onto the Chatham House wifi and search desperately for Silk Road. To address those issues – plenty of questions there – David Anderson.

David Anderson

It's a fascinating book, certainly increased my vocabulary – although I'm not going to confess to doxing a cam girl or any of the other things that Jamie tells us about. It's not a book about terrorism but it prompted plenty of reflections in me about some extremely topical issues in counterterrorism. I thought I might just very briefly outline three of those.

The first is the question of whether laws devised for the real world still work on people who, like so many of the people that Jamie met, effectively live in a digital world. One of the things that I learned from the book – I probably should have known it before – is that among the many online influences cited by Anders Breivik, the Norwegian terrorist, in the manifesto that he published on the day of his murders was the work of Jeremy Clarkson. In a world where people can associate and be influenced by each other online, to the extent that they can, is there any point in seeking to restrain the personal associations of people who are suspected of terrorist offences?

This has come up recently in the context of the debate that's going on at the moment within the coalition as regards the future of control orders, or TPIMs as they're now called – Terrorism Prevention and Investigation Measures. Under the Labour government it was possible to relocate people under control orders, send them to Norwich or Gloucester or some similar place so that they couldn't meet with their associates in London, for example. The debate currently going on concerns whether it's necessary to reintroduce that power or whether we can do just as well without.

One of the arguments against doing it which has been presented to me is, well, there really isn't any point. These people can do so much online. What are you actually going to achieve by preventing their physical association? I was reminded of this very much last year. I was invited to tea by Abu Qatada just before he was deported. As he spoke to me through an interpreter, with Arabic-language television blaring in the background, I realized that although he'd lived in the country since 1992, the relationships that mattered – the communications that mattered – were really in a different world. It wasn't the world of Stanmore, it was a more international world than that. Which again makes one think of the importance we've attached to extradition, to deportation, to getting rid of people physically out of the jurisdiction. Are we perhaps hitting the wrong targets? Do we need to adapt as the world gets more digital?

Second issue I wanted to raise was what one might broadly call censorship – the extent to which it's reasonable for the state to discourage or seek to prevent people from reading things and viewing things. You might remember that there was recently a propaganda video produced by the so-called Islamic State, depicting the beheading of James Foley. When that video was released a few weeks ago, the Metropolitan Police put out a statement which is worded as follows: 'We would like to remind the public that viewing, downloading or disseminating extremist material within the UK may constitute an offence under terrorism legislation'.

Whether or not it's correct – and I leave aside the question of whether it's right in law to say that viewing a video of this kind could have been a criminal offence, or to imply that – a couple of questions occur to me. The first is: are constraints of that kind futile? Jamie makes the point very strongly in his book that the encrypters seem to have the upper hand. It may be a little cumbersome but there seem to be ways of encrypting things. People have suggested that any attempt to govern what people look at online is simply futile when you have the dark net and you have methods of encryption.

Or, on the other hand, is that a counsel of despair? A bit like saying there's no point keeping fingerprints because somebody invented the glove, and if you're clever enough to remember to put a glove on, you're never going to leave any fingerprints. The reality is an awful lot of criminals are too stupid or too careless to bother with the gloves and the fingerprints enable them to be caught. But room for debate there.

We also have to look, I think – more than 300 years after we ended the censorship of the written word – at the activities of the Counter Terrorism Internet Referral Unit within the offices of the Metropolitan Police. We're told privately that in its first four years, it secured the taking down of more than 25,000 pieces of illegal terrorist content. Well, what criteria are being applied? How successful was it in taking down that content? How much of it may have popped out elsewhere? I don't express any views on that but I think an issue for consideration.

The second point is: are these laws, even if they are not futile, if they can achieve something, are they actually desirable? Is it right that we should be preventing or strongly deterring people from viewing, for example, beheading videos? Can we still defend, where terrorist propaganda is concerned, the old liberal idea of the marketplace of ideas, where the good will drive out the bad, where bad speech is met with good counter-speech, and the counter-speech triumphs.

I'd add to that the argument that it's necessary to see what your enemy is saying in all its unvarnished glory if you are properly to assess what your enemy is about. You've had people like Anjem Choudary in this country actually denying that the so-called Islamic State is engaged in the slaughter of civilians. If you sanitize the web or attempt to sanitize the web, to the extent that somebody wants to check for themselves can't actually find any very bad stuff, do you risk making them look better than actually they are? Certainly there is some German jurisprudence along those lines which I find very interesting, saying no, you can't censor party election broadcasts because they convey an anti-constitutional message, because if you did that, people wouldn't realize that that party stands for the subversion of the constitution.

I think my third point is what you may loosely call surveillance. I put in a plug here for the fact that I'm engaged at the moment on a review of investigatory powers, which the three political parties have asked me to do by the general election. There are still, I think, just over three weeks left for written submissions if anybody is thinking of making one. You'll find the details on the website of the Independent Reviewer of Terrorism Legislation.

But there are some very basic questions there. One of them is, it seems to me: does privacy, or do the interests of privacy, require there to be what a judge once called an 'Alsatia where the King's writ does not run'? Is it right that there should be areas in which one can communicate with complete freedom and complete knowledge that one will not be overheard? If so, should that anonymous space be digital or should it be analog, or should it be both?

When the government was promoting the Communications Data Bill a couple of years ago, a bill which eventually fell amid disagreement within the coalition, they were saying if, given proper safeguards, you can access the details of emails and the details of telephone conversations, surely it must be right that you can access the details of Facebook communications, communications through computer games. Otherwise you're giving criminals and terrorists a failsafe way of talking to each other. I think that logic would have a lot of force for a lot of people.

But if it's acceptable to do that and to close down the digital Alsatia, why should it not also be acceptable to commission a next-generation drone which can hover at 60,000 feet and pick up every conversation going on in every bedroom, in every house in the country? Of course, one would have excellent safeguards. One could only listen to the conversations if you had reasonable suspicion, and if you had nothing to hide, you would have nothing to fear. One can also see the very great benefits that such a system would have in terms of, for example, improving conviction rates for domestic violence. They would go through the roof and that scourge of society would be much diminished.

I sense less people would be favourable to that and more people would feel that because it's analog, it's between human beings in real space and real time, it's less reasonable to exercise that capacity to listen to it. But I'd like to know why. In particular, talking to you young people, I'd like to know whether there's a generational aspect to this. Some people have suggested to me that people of my generation are much more sanguine about allowing others to access their digital communications because we've always thought of that as a bit of an add-on to our primarily analog lives. But for the young, particularly very young, who take their medical advice online, conduct relationships online, there may be something more sacred about online communications or some forms of online communication. Anything in that or a red herring? I would like to know. I think that's enough from me.