AN INTERVIEW WITH CASPAR BOWDEN

Caspar Bowden (cb@fipr.org) is the author of a recent DLTR article, Closed Circuit Television for Inside Your Head: Blanket Traffic Data Retention and the Emergency Anti-Terrorism Legislation. He is the Director of the Foundation for Information Policy Research (http://www.fipr.org), an independent non-profit think-tank that undertakes research on the interaction between information technology and society, technical developments with significant social impact, and public policy alternatives. He was formerly a consultant specializing in Internet security and e-commerce, senior researcher of an option-arbitrage trading firm, a financial strategist with Goldman Sachs, and chief algorithm designer for a virtual reality software house. We interviewed Mr. Bowden about combating terrorism in Europe and other issues related to European cyber-policy, such as the success of a European Internet and Information policy.

****

You argue in your article, Closed Circuit Television For Inside Your Head, that the UK's anti-terrorism legislation may harm the security, privacy, and freedom of expression of law-abiding citizens and that it will likely be ineffective in detecting or deterring terrorist communications. How would you modify the UK's legislative framework to increase the likelihood of its effectiveness and lessen the potential for civil liberties abuses?

The basic argument is whether machinery to put the entire population under computerized surveillance is compatible with human rights in a democratic society, and also whether such measures are likely to be effective in stopping terrorism, which together with drug trafficking, money laundering and child pornography, is the most often cited justification.

The argument is very complex, involving the arcane concept of "steganography" (information hiding), but overall takes the form of a reductio ad absurdum. The unpalatable truth is that both terrorist command structures and operational cells can use practical and effective communications tradecraft to elude detection altogether, even if the resources hitherto employed by the National Security Agency (NSA) against external enemies were turned inward. There is thus no point in proceeding down that path to protect against terrorism, although such capabilities could be profoundly dangerous to democratic society in other ways.

An alternative approach, which is by no means a perfect substitute for the illusory omniscience sought by the authorities, is to by-pass encryption and other security measures by developing sophisticated software viruses, used in conjunction with robust traditional methods of covert search and entry and installation of physical devices such as keystroke loggers.

Unlike blanket retention of traffic data (or the discredited idea of key-escrow), these techniques at least stand a chance of working effectively, where the target's platform can be identified or reached indirectly. They are also preferable from the civil liberties point of view, because there is an intrinsic incentive to minimize their deployment to reduce the risk of compromise. In the US, the application of existing law to key-logging was recently tested in the "Scarfo" case,[1] but important questions remain on whether targets have a constitutional right to be notified eventually.

The UK has no legislation explicitly addressing use of these techniques, although existing powers governing microphone bugs could be shoe-horned to fit. However, these techniques will need oversight and supervision of unprecedented stringency, because false evidence could easily be concocted, and arguably they should thus only be used for gathering intelligence. The legalistic UK oversight regime is a "concrete lifejacket" - the deliberately vague formalities could all be adhered to, but flagrant and massive abuse could still disappear without trace.

Therefore FIPR is far from endorsing such an approach, because oversight mechanisms are so deficient, nevertheless we did predict some years ago that capabilities such as the FBI's "Magic Lantern" would surely be developed.

Is the UK approach to combating terrorism similar or dissimilar to the approach being taken in the US? Is the US approach any better?

Since WW2, there has been extremely close intelligence sharing of communications surveillance for national security. The main difference is that there are categorical safeguards for US citizens, whereas UK legislation provides nothing comparable for British subjects. Under the USA/PATRIOT Act which was rushed through with cursory debate after 9/11, the NSA is empowered to trawl through domestic communications for much broader purposes than before.

[1] U.S. v. Scarfo, 180 F. Supp. 2d 572 (D.N.J. 2001).

The RIP Act 2000 had already given even more drastic powers to GCHQ, the UK equivalent to NSA about one seventh the size, but it is some way from having the technical capability or carrier's co-operation for implementation. It can be read as a 10-year plan for a domestic surveillance infrastructure that can hunt for targets dynamically rather than a capability to trawl everything simultaneously.

The UK passed further draconian "anti-terrorist" legislation following 9/11, but which is equally applicable to minor crimes. The most disturbing aspect is a philosophical shift which has been virtually unreported, dubbed the "M&M-principle". Previous anti-terrorist legislation, for example dealing with Northern Ireland, has defined especially severe powers for especially severe crimes. However the UK government now literally says that since investigating theft of a bag of M&Ms *might* lead to uncovering an al Qaeda terrorist cell, even the most extreme powers must be available to pursue the most minor crimes. They say matching personal details from separate databases will not be used for “fishing expeditions”, but in the same breath argue they must be allowed to piece together a “jigsaw” – a distinction without a difference in a computer context. At the same time, it likes to claim that these powers are fully conformant with human rights, since they must implicitly be exercised proportionately. The trouble is that they are also mostly exercised secretively, so complaint and redress is in most cases unobtainable. Thus they have substituted an explicitly graduated framework of threat and response supervised by judges, for an infinitely malleable executive prerogative. The irony is that this innovation was the grand achievement of bien-pensant civil liberties lawyers, who naively ignored how the government machine would implement their proposal.

How are other European countries seeking to combat terrorism? Has the EU sought to coordinate a European-wide approach?

There was agreement reached on a Europe-wide arrest warrant, but for purposes much broader than terrorism (including "harmful" speech), and heavy pressure is being applied by the UK, France, Netherlands and Belgium to abolish existing protections. In fact President Bush wrote to the President of the EU Commission requesting mandatory traffic data retention, which seemed odd since the US is not proposing comparable legislation of its own. However, unlike EU citizens, US citizens do not have the safeguard of data protection legislation which prohibits blanket stockpiling of data for surveillance, nor the right to "subject-access" to discover what information is held about them by the private sector. For example, major US telcos are rumoured

never to have thrown away any call record since billing systems were unified in the mid-80s. How much data US ISPs keep is unknown and in most cases the customer has no contractual right to know.

The Council of Europe (CoE) (an entirely separate entity from the EU), because it has zero transparency or public accountability, has been the international forum of choice for surveillance hawks. The international criminal law of cyberspace was written by a dozen appointed "experts" working in secret for four years – we still don't know their names. Amongst other excessive powers, the CoE Convention on Cybercrime mandates a capability to stream highly sensitive traffic data across national boundaries in real-time, over-riding data protection and human rights due process.

Could you briefly describe the European cyber-policy NGO scene? Who are the key players? How do they interact at the national, European and international levels?

There are at least fifty different grass-roots European cyber-NGOs, almost none professionally staffed or funded, and the only co-ordination between them has been through GILC (the Global Internet Liberty Campaign), and APC (Association for Progressive Communications). In France, the joke goes that if you want to start an NGO, then you'd better get the government to help you. In Britain, old legalistic NGOs have a sclerotic conception of civil liberties which finds cyber-issues unintelligible. Germany has a strong hacker-rights culture, but corresponding difficulties engaging with mainstream institutions.

Is there a democratic deficit in European civil society tech policy? How does this differ from the United States? Are there any steps that are being taken, or should be taken, to reduce the democratic deficit?

The democratic deficit is massive. Some of the key NGO players have recognized this for a long time, but lacking the philanthropic resources common in the US, or the leverage to get core funding from the EU like the consumer lobby, several past attempts to bootstrap a coalition have atrophied. Although there have been patchy successes at national level (e.g. ameliorating amendments to RIP), at the European level the result has been disastrous. Law-enforcement agencies have had a clear field to dictate absurd wish-lists, unchallenged by independent expert scrutiny. Such NGO representations as have been made to the EU Parliament and Commission

have been ineffectual, ignored or misunderstood. Much of the EU apparat are still hostile to NGOs, and that which is sympathetic is super-cautious.

George Soros' OSI and the Markle Foundation providing early funding of East European cyber-rights projects, but nothing for western Europe. The assumption seemed to be that in mature liberal democracies, nothing really bad or stupid would happen. Well, it has, and it's getting worse.

Have European governments been successful in making Internet and information policy? Why or why not?

The EU institutions really only "got" the Internet around 1998, having previously been wedded to an obsolete 80's notion of "telematics" (low-bandwidth smart networks operated by telcos). Since then much hot-air has been ventilated at EU summits, but the machinery has such inertia that it always lags years behind. A good example was the EU Commission attempt to push local-loop unbundling across Europe, which began to bite just as the dotcom crash blew away the rivals to the incumbents. EU research programmes are underfunded and so bureaucratic that leading researchers simply don't apply, and the "deliverables" are usually a mediocre PowerPoint show aptly nick-named Euro-dreck.

Is online banking secure? How can customers protect themselves? Are the initiatives being undertaken in the UK and the EU satisfactory? Why or why not?

The truth is that online banking has always been secure, relative to other risks - the main issue is regulatory not technical. Banks lobbied hard but unsuccessfully to offload uncontrollable liabilities onto the customer. Arguments about key-length were for a time a useful stick with which to beat export control and escrow policy, but now the game has moved on.

Computers can never be made secure with software alone (for example a virus or bug could be used to steal your password or decryption key), but the risks are usually manageable. But attempting to make all hardware secure begs the question "secure for whom"? The industry is developing a specification for new PCs which could be interrogated remotely to establish whether the user's machine is "trustworthy", and refuse service otherwise. Enormous power would be concentrated in a few levers of control, and this could tilt the market to a degree where the

freedom to run any software you want will effectively be lost. Such locked-down hardware could make outlandish copyright or surveillance laws enforceable (although it still could not stop terrorism). That is why the Internet community in Europe is just astounded and horrified at Sen.Hollings' CBDTPA Bill. The TrustedPC initiative has an extraordinarily naïve and limited conception of user privacy. It is precisely the kind of architectural shift that Lawrence Lessig warns us could transform the Internet into a control freak's paradise, unless an entrenched democratic consensus to resist this develops. But in the UK and I suspect also in the US, only about 1% of the legislature has ever programmed a computer, so these arguments are never articulated. NGOs may have to hold the line for a generation before that changes.

Interview by: Joseph Goodman