Director of British rights group Cage convicted for refusing to reveal mobile phone and laptop pass codes

Steve James
4 October 2017

The international director of advocacy group Cage, Muhammed Rabbani, has been convicted under Schedule 7 of Britain's draconian Terrorism Act for refusing to reveal pass codes for his mobile phone and laptop.

Rabbani was convicted last month at Westminster Magistrate's Court by Senior District Judge Emma Arbuthnot for "willfully obstructing" a stop and search. He was ordered to pay court costs and conditionally discharged for 12 months. He intends to appeal.

Cage was set up in 2003, as CagePrisoners, to highlight the "plight of the prisoners at Guantanamo Bay and other detainees held as part of the War on Terror." Among Cage's other directors is former Guantanamo prisoner Moazzam Begg.

Rabbani was held November 2016 at Heathrow Airport in London on return from Qatar. He was questioned for three and a half hours before being handcuffed, arrested and held for nine hours. His laptop, phone and a USB stick were seized.

In a statement made in May this year, Rabbani made clear his principled stand:

"I considered that although the police were in law entitled to ask questions so that they could satisfy themselves I was not engaged in terrorist activity, that did not justify my in addition being required to expose all the sensitive contents of my phone to being copied and undoubtedly disseminated not just to police but to intelligence services and possibly elsewhere in the world—an unjustifiable, uncontrolled acquisition of material."

During his trial Rabbani explained the sensitive nature of his case as one "involving the US against an individual who was allegedly tortured over the course of 12 or 13 years in US custody." He went on, "There were around 30,000 (documents) which I was especially uncomfortable handling and I felt an enormous responsibility to try and discharge the trust that was given to me."

Under Schedule 7, police and immigration officials can detain and question any person passing through border controls under the pretext of determining whether they are involved in terrorism. In practice, the schedule is a dragnet to pry on the affairs of travellers, particularly those whose activities come into conflict with the nefarious activities of the military-intelligence complex.

According to *Middle East Eye*, between 2015 and 2016 under Schedule 7 561,660 people were asked screening questions, 28,083 examinations were carried out, 10,000 intelligence reports were filed and 1,677 had the contents of their phones downloaded. Yet only 0.02 percent of stops led to an arrest, even less to charges.

The most notorious use of Schedule 7 was the arrest in 2013 of David Miranda, also at Heathrow, when he was carrying electronic files relating to material leaked by former US National Security Agency contractor Edward Snowden exposing mass surveillance by US and UK spy agencies. Miranda was threatened with jail and his laptop, camera, cell phone and other personal items seized and trawled for data.

Rabbani's case underscores the significance of recent investigations into the massive extent of mobile phone surveillance in Britain by local police forces.

Extensive use of smart phones means that, in addition to allowing voice and text messages to the targeted, vast amounts of personal data, either stored on smart phones or accessed from them, can potentially be collected.

So-called "IMSI-catchers" [International Mobile Subscriber Identity-catchers] are portable devices that masquerade as mobile phone cell towers to which mobile phones connect for voice calls and data transmission and reception. By deploying an IMSI-catcher in an area, its

owner can potentially identify every active mobile phone within an area of up to eight square kilometres via its unique subscriber identity and approximate its location. Police operators can develop a live map of every active phone user in an area. They can also listen to phone calls and read text messages.

In 2016, an investigation by the *Bristol Cable* media cooperative revealed that, as well as London's Metropolitan Police, as many as five other local forces were using IMSI-catcher technology. British police forces have consistently refused to report any use of the devices, but by deciphering an acronym, CCDC, in police procurement records and published minutes as Covert Communications Data Capture, investigators concluded Avon and Somerset, West Midlands, South Yorkshire, Staffordshire, Warwickshire and West Mercia police forces all had purchased CCDC technology. The devices purchased by West Mercia and Staffordshire at least were compatible with 4G mobile networks.

The deployment of IMSI-catcher tools in a locality allows police forces to identify individuals attending a demonstration, while monitoring their communications. It allows eavesdropping on private phone calls and messages, for example between lawyers and clients, or journalists and their sources.

Efforts by rights organisation Privacy International to use Freedom of Information requests to clarify the extent of IMSI-catchers by police forces have been rejected by every police force contacted on grounds of "national security".

Other technologies are in use.

Further investigations by the *Bristol Cable*, and the *Ferret,* another investigative group based in Scotland, focused on the widespread deployment of easy to use mobile phone cracking devices. As of January this year, some 28 local police forces in the UK, as well as the Home Office, had contracts with Israeli company Cellebrite whose most popular product is the Universal Forensic Extraction Device (UFED).

The UFED is a portable gadget that can quickly extract mobile phone pass codes allowing access to personal text messages, emails, photos, videos, GPS location data by attaching the target mobile phone to the UFED and following straightforward documented procedures.

Cellebrite also claim that data stored in encrypted apps, passwords to cloud services and third-party apps can be extracted, giving access to a vastly expanded data hoard. In all, the company claims that data can be pulled from some 21,374 phone models, including most iPhone and Android based devices.

Further investigation by the *Cable* concluded that North Yorkshire police is one of the forces deploying UFEDs and that no audit trail had been left for 50 percent of a sample of its mobile phone data extractions. This means that there is no means of confirming whether searches were even legal or what happened to the extracted information. The same investigation found that only 26 percent of searches were regarding "serious crime type, for example sexual offences and murder cases."

Hundreds of police officers are being trained in the use of UFED and similar devices. West Yorkshire Police is reported to have trained 150 officers on how to examine mobile phones, for offences ranging from traffic violations to assault. Durham Police reported that 90 percent of searches are carried out by local officers, while the City of London reported that searches are generally undertaken by "frontline officers... generally in the first custody detention period."

The scale of data gathering was clarified in another article in the *Ferret* which, based on Freedom of Information requests, reported that over the last three years Police Scotland alone had successfully extracted data from 35,973 phones and 16,587 computers. The *Ferret* notes that police can legally seize and analyse electronic devices belonging to anyone detained, or arrested, for any reason. Evidence is admissible in court even if the data is obtained without the owner's permission. Police Scotland have 56 staff members dedicated solely to analysing mobile devices, with more being trained every year.

People voluntarily giving consent to their phone being examined may not be aware of the extent of personal data being handed over. Police Scotland procedure states, "Only information held on the mobile telephone or SIM card when it was seized can be retrieved during the course of an examination," but this can be overcome if the device owner gives authorisation for the examination or if the police obtain a warrant.