Written by **Raven Clabough** on February 21, 2012

Big Brother Returns to Orwell's England

It seems the U.S. government is not the only one sporting a Big Brother demeanor. The British government is now revisiting previously considered plans to create databases that would enable spy agencies to monitor emails, phone calls, and text messages as well as websites visited by everyone in the United Kingdom. Entitled the Communications Capabilities Development Programme (CCDP), the scheme would be set up under anti-terrorism laws, in much the same way the PATRIOT Act functions in the United States. UK officials contend that its goal is to closely monitor suspects before the 2012 London Olympics in July.

The proposal — conceived by MI5 (Military Intelligence 5, a government agency dealing with domestic threats), MI6 (which combats overseas threats), and the Government Communications Headquarters (GCHQ) — could be announced as early as May. Those agencies would be given access to records kept by companies such as Vodafone and British Telecom. British spy agencies would be permitted not only to evaluate all communications exchanged, but also to match Internet browsing histories to IP addresses.

Under the plan, communications networks would be required to store the data for a full year. The proposal includes even social networking sites such as Facebook and Twitter, as well as gaming sites.

The Telegraph explains:

> For the first time, the security services will have widespread access to information about who has been communicating with each other on social networking sites such as Facebook.
>
> Direct messages between subscribers to websites such as Twitter would also be stored, as well as communications between players in online video games.

Naturally such a proposal has drawn the ire of freedom-lovers in England. Jim Killock, executive director of the Open Rights Group, a civil liberties campaign organization, declared, "This would be a systematic effort to spy on all of our digital communications. No state in history has been able to gather the level of information proposed — it's a way of collecting everything about who we talk to just in case something turns up."

Gus Hosein, of Privacy International, pointed out,

> This will be ripe for hacking. Every hacker, every malicious threat, every foreign government is going to want access to this. And if communications providers have a government mandate to start collecting this information they will be incredibly tempted to start monitoring this data themselves so they can compete with Google and Facebook.
>
> The internet companies will be told to store who you are friends with and interact with. While this

> may appear innocuous it requires the active interception of every single communication you make, and this has never been done in a democratic society.

The Open Rights Group is now circulating an online petition against the controversial program, calling it "pointless," "expensive," and "illegal." The petition explains, "This Kafka-esque 'Intercept Modernisation Plan,' was stopped near the end of the last government, but was quietly revived in the 2010 Spending Review (read more here) as the 'Communications Capabilities Development Programme.' Now, closed-door discussions have been revealed: legislation will be proposed in May."

Those who sign the petition are putting their name to the following statement: **"**I do not want the government to try to intercept every UK email, Facebook account and online communication. It would be pointless — as it will be easy for criminals to encrypt and evade — and expensive. It would also be illegal: mass surveillance would be a breach of our fundamental right to privacy. Please cancel the Communications Capabilities Development Plan."

As alluded to earlier, this is not the first time the British government has considered such an extreme proposal. In 2008, the government announced its intent to launch a massive central database that would have gathered information on every text, email, and phone call circulated in the United Kingdom, as well as every website visited. That plan, called the "Interception Modernisation Programme," would have permitted the GCHQ, where the Signal Intelligence (SIGINT) functions, to place a "live tap" on every electronic communication in Britain under the guise of preventing terrorism.

The proposal sparked such a harsh public outcry that the British government indicated that it would cut back on some of its plans. Britain's Home Secretary Jacqui Smith announced that there were "absolutely no plans for a single central store" of communications data.

But even as civil liberties advocates in Britain celebrated their victory of foiling the government's plans to implement such a program, new laws were being passed that required ISPs to store email and Internet details for 12 months.

The *London Times* and *The Register* then exposed details of a secret mass Internet surveillance project known as "Mastering the Internet" (MTI). That costly system was enacted by the GCHQ with the help of the American global aerospace, defense and technology firm Lockheed Martin, and the British IT company Detica. Lockheed Martin was reported to have made £200M from the deal.

According to *The Register*, "The system — uncovered today by *The Register* and *The Sunday Times* — is being installed under a GCHQ project called Mastering the Internet (MTI). It will include thousands of deep packet inspection probes inside communications providers' networks, as well as massive computing power at the intelligence agency's Cheltenham base, 'the concrete doughnut'."

Sources close to the project at the time indicated that contracts had already begun to be handed out to private sector partners.

One said: "In MTI, computing resources are not measured by the traditional capacities or speeds such as Gb, Tb, Megaflop or Teraflop… but by the metric tonne!.. and they have lots of them."

At the time, over 300 ISPs and telecommunications firms fought the plans, which they saw as invasions of privacy.

Current English law permits the government to intercept communication only when a warrant has been obtained and signed by the Home Secretary or a Minister of equivalent rank, and only in the case of an individual who is the subject of a police or security service investigation; however, if the new proposed

program were to be implemented that would change. Black-box probes would be placed at traffic intersections with Internet service providers and telephone companies, permitting spies to monitor the communications of every person in the country without a warrant.

Britain already has a law in place that allows the government to access what should be the private records of every Internet provider in the country: the Regulation of Investigatory Powers Act. But the new program would provide every Internet user a unique ID code so that their data might be stored in one place. The government and police would then have access to the data on request.

A similar program may be established in the United States under the Protecting Children from Internet Pornographers Act (PCIPA), which would force Internet providers to store information on all their customers and share that information with the government and law enforcement when told to do so.

While privacy experts have bemoaned the PCIPA as a "stalking horse for a massive expansion of power," lawmakers have touted the bill as a positive step toward keeping children safe.

Photo: A model of the British Government Communications Headquarters (GCHQ).