

# Taking Britain's Communications and Intelligence Agency (GCHQ) to Court: The Legal Claim Against Surveillance

By [Dr. Binoy Kampmark](#)

Global Research, July 07, 2014

Region: [Europe](#)

Theme: [Intelligence](#), [Law and Justice](#)

*People have a fundamental right to communicate with each other free from pervasive government surveillance. The right to communicate, and the ability to choose to do so secretly, is essential to the open exchange of ideas which is a cornerstone of a free society. Devin Theriot-Orr, Riseup.net, July 2014*

*"GCHQ is an intelligence and security organisation, working to keep Britain safe and secure in the challenging environment of modern communications.*

*Today, we address a range of modern demands, dealing with threats from terrorism, the spread of nuclear weapons and the resolution of regional conflicts around the world, as well as protecting the economic prosperity of the UK. We work closely with colleagues from other government departments, UK armed forces serving abroad, and with our partners in the intelligence community, MI5 and Secret Intelligence Service (MI6).*

*We work to the Foreign Secretary and are subject to scrutiny from Parliament, two senior judges and the Investigatory Powers Tribunal on the legality, necessity and proportionality of our work. We are proud of being an organisation of high ethical standards and culture, embedded in the framework of British law.*

*We are a secret organisation. We cannot publish all that we do – it would compromise our operations and our capabilities. But I hope that you will get a picture of the work we do, the challenges we face and the kind of people we are. (Iain Lobban, GCHQ Director, [Welcome to GCHQ](#), GCHQ website*

Can you take a signals intelligence agency to court, or at the very least, something approximating to it? Various bodies have been putting their minds together, considering the formidable obstacles, the endless riddling hoops. Last week, they lodged a claim<sup>1</sup> before Britain's Investigatory Powers Tribunal against both the UK's GCHQ and the Foreign and Commonwealth Office (FCO), arguing that the former's targeting of Internet service providers was illegal, destructive and retarding of the goodwill such providers rely upon.

Ultimately, such interference on the part of GCHQ cripples the very functioning of the Internet, a true violation of associated freedoms of use. As Privacy International's Deputy Director, Eric King, explains, "These widespread attacks on providers and collectives undermine the trust we all place on the internet and greatly endangers the world's most powerful tool for democracy and free expression."

The claimants are a varied, international assortment, though it is worth noting that they are far from the premier league of ISPs. The collective exudes internet activism and a bookish but important concern for liberties, including RiseUp (US), GreenNet (UK), Greenhost (Netherlands), Mango (Zimbabwe), Jinbonet (South Korea), May First/People Link (US), the Chaos Computer Club (Germany), and Privacy International. They are using the services of Bhatt Murphy lawyer Shamik Dutta, and Blackstone Chamber's Ben Jaffey and Tom Cleaver.

The specific legal details won't make the legal layman's eyes glaze over. They should, however, chill and anger the blood in equal measure. They have privacy implications not merely for the users of the ISPs in question, but the staff who work for those companies.

The alleged breaches of such conduct on the part of GCHQ suggest something fundamental to the everyday user of ISPs: the violation of Article 1 of the First Protocol, and Articles 8 and 10 of the European Convention on Human Rights (ECHR). Such provisions, in addition to affirming rights of free speech and privacy, make it clear that any interference is only warranted "in accordance with the law", "prescribed by law", or "subject to the conditions provided for by the law" and must be consistent with the principles of a democratic society and proportionate to such ends.

The source of the claim lay in articles published in *The Intercept* and *Der Spiegel*. Specific instances include the targeting of employees of Belgacom, who were affected by malware via an attack termed "Quantum Insert". The basis of that was, unsurprisingly, to gain access to material pertaining to the infrastructure network. According to the report, GCHQ were "on the verge of accessing the Belgians' central roaming router." In doing so, the agency would have been able to stage complex "Man in the Middle" (bypassing encryption software) attacks on smartphone users.

The viral and biological metaphor here is never far away - much of the capabilities which concern the claimants centre on the rendering of communications infrastructure vulnerable to infection. Denude the network; gather the information. "Man on the Side", for instance, involves the covert injection of data into, as Privacy International's statement explains, "existing data streams in order to create connections that will enable the targeted infection of users."

According to the claim, the attack of network infrastructure "enables GCHQ to undertake a range of highly invasive mass surveillance activities, including the application of packet capture (mass scanning of internet communications); the weakening of encryption capabilities; the observation and redirection of internet browsing activities; the censoring or modification of communications en route; and the creation of avenues of targeted infection of users' devices."

Again, GCHQ has shown that the banal and the irrelevant are worthy of its intrusive efforts. Data is data, and it must be snatched, however disproportionate the measures. As the claim states,

"What is more concerning is that the conduct set out... has no proper justification. Each of the Claimants is a responsible and professional internet service provider. None has any interest in supporting terrorist activity or criminal conduct."

Discrimination has little to do with it, for the modern fetish of mass surveillance is that

something, somewhere, is relevant.

As Cedric Knight of GreenNet explained to RT (Jul 3), "It seems that GCHQ has been deliberately targeting the ordinary technical staff who tried to protect network security, to try to find personal weaknesses and the weakness in the security systems they put in place."

There are big questions that remain, those teething problems of taking public interest cases before a tribunal without necessarily proving tangible damage. The claimants admit that they may or may not have been affected, but that the interactive nature of the Internet and such surveillance suggests a high probability that they have been.

This has been the greatest boon for intelligence services - that hallowed insistence that those who seek judicial remedy prove actual harm. Then there is the question about how far a body such as the IPT will go. According to Knight, the IPT "doesn't give much details of its investigations if any at all."

GCHQ may get a slap on its capacious wrist, but that it should get a slap at all might be a miracle. The claimants are aiming high: a declaration that GCHQ's intrusive conduct is unlawful; an order of destruction of "any unlawfully obtained material" and an injunction restraining further unlawful conduct. As Knight argues, a first step in such an action is to have an open hearing of such claims at all.

*Dr. Binoy Kampmark was a Commonwealth Scholar at Selwyn College, Cambridge. He lectures at RMIT University, Melbourne. Email: [bkampmark@gmail.com](mailto:bkampmark@gmail.com)*

The original source of this article is Global Research  
Copyright © [Dr. Binoy Kampmark](#), Global Research, 2014

---

[Comment on Global Research Articles on our Facebook page](#)

[Become a Member of Global Research](#)

Articles by: [Dr. Binoy Kampmark](#)

**Disclaimer:** The contents of this article are of sole responsibility of the author(s). The Centre for Research on Globalization will not be responsible for any inaccurate or incorrect statement in this article. The Centre of Research on Globalization grants permission to cross-post Global Research articles on community internet sites as long the source and copyright are acknowledged together with a hyperlink to the original Global Research article. For publication of Global Research articles in print or other forms including commercial internet sites, contact: [publications@globalresearch.ca](mailto:publications@globalresearch.ca)

[www.globalresearch.ca](http://www.globalresearch.ca) contains copyrighted material the use of which has not always been specifically authorized by the copyright owner. We are making such material available to our readers under the provisions of "fair use" in an effort to advance a better understanding of political, economic and social issues. The material on this site is distributed without profit to those who have expressed a prior interest in receiving it for research and educational purposes. If you wish to use copyrighted material for purposes other than "fair use" you must request permission from the copyright owner.

For media inquiries: [publications@globalresearch.ca](mailto:publications@globalresearch.ca)