

HUMAN RIGHTS WATCH

Audrey House
16-20 Ely Place
London EC1N 6SN UK
Tel: +44 (0)20 7713 2766
Email: mephamd@hrw.org

Kenneth Roth, *Executive Director*
Michele Alexander, *Deputy Executive Director, Development and Global Initiatives*
Carroll Bogert, *Deputy Executive Director, External Relations*
Jan Egeland, *Europe Director and Deputy Executive Director*
Iain Levine, *Deputy Executive Director, Program*
Chuck Lustig, *Deputy Executive Director, Operations*

Walid Ayoub, *Information Technology Director*
Emma Daly, *Communications Director*
Barbara Guglielmo, *Finance and Administration Director*
Peggy Hicks, *Global Advocacy Director*
Babatunde Olujobi, *Deputy Program Director*
Dinah PoKempner, *General Counsel*
Tom Porteous, *Deputy Program Director*
James Ross, *Legal and Policy Director*
Joe Saunders, *Deputy Program Director*
Frances Sinha, *Human Resources Director*

PROGRAM DIRECTORS

Brad Adams, *Asia*
Joseph Amon, *Health and Human Rights*
Daniel Bekele, *Africa*
John Biaggi, *International Film Festival*
Peter Bouckaert, *Emergencies*
Zama Coursen-Neff, *Children's Rights*
Richard Dicker, *International Justice*
Bill Frelick, *Refugee Policy*
Arvind Ganesan, *Business and Human Rights*
Liesl Gemholtz, *Women's Rights*
Steve Goose, *Arms*
Alison Parker, *United States*
Graeme Reid, *Lesbian, Gay, Bisexual and Transgender Rights*
José Miguel Vivanco, *Americas*
Sarah Leah Whitson, *Middle East and North Africa*
Hugh Williamson, *Europe and Central Asia*

ADVOCACY DIRECTORS

Philippe Bolopion, *United Nations*
Kanae Doi, *Japan*
Jean-Marie Fardeau, *France*
Meenakshi Ganguly, *South Asia*
Cameron Jacobs, *South Africa*
Lotte Leicht, *European Union*
Tom Malinowski, *Washington DC*
David Mepham, *United Kingdom*
Wenzel Michalski, *Germany*
Juliette de Rivero, *Geneva*

BOARD OF DIRECTORS

Jane Olson, *Chair*
Bruce J. Klatsky, *Vice-Chair*
Sid Sheinberg, *Vice-Chair*
John J. Studzinski, *Vice-Chair*
Karen Ackman
Jorge Castañeda
Geoffrey Cowan
Tony Elliott
Hassan Elmasry
Michael G. Fisch
Michael E. Gellert
James F. Hoge, Jr.
Betsy Karel
Wendy Keys
Robert Kissane
Joanne Leedom-Ackerman
Susan Manilow
Kati Marton
Barry Meyer
Pat Mitchell
Joel Motley
Joan R. Platt
Neil Rimer
Victoria Riskin
Amy L. Robbins
Shelley Rubin
Kevin P. Ryan
Jean-Louis Servan-Schreiber
Darian W. Swig
John R. Taylor
Catherine Zennström

Robert L. Bernstein, *Founding Chair, (1979-1997)*
Jonathan F. Fanton, *Chair (1998-2003)*



HRW.org

The Rt. Hon William Hague MP
Secretary of State for Foreign and Commonwealth Affairs
Foreign and Commonwealth Office
King Charles Street
SW1A 2AH

1 July 2013

Dear Foreign Secretary

RE: Data surveillance claims and protecting the right to privacy

Human Rights Watch is seriously concerned by recent reports suggesting that the UK intelligence agency GCHQ has intercepted and collected vast amounts of internet and phone data from people living in the UK and other countries.

According to reports in the Guardian newspaper, GCHQ has accessed enormous quantities of data travelling from North America to and through the UK and has shared this data with the US National Security Agency (NSA). The data is said to include recordings of phone calls, e-mail contents and data on the use of websites and social media. The reports suggest that the content of the data is generally stored for up to three days, and that metadata (which for the internet includes information identifying users, their locations and their searches) for up to 30 days. It has been further suggested that analysts for GCHQ and NSA then filter through the data, searching for information that is of interest or use to them.

In response to these allegations you have defended the nature of the UK's intelligence sharing with the US and said that the intelligence work of both countries operates under the rule of law, stating that in "some countries secret intelligence is used to control their people - in ours it only exists to protect their freedoms". You have also asserted that it is the practice of successive UK governments not to talk publicly about the detail of intelligence matters or to confirm or deny any aspects of leaked information. Human Rights Watch believes that both claims - that the existing legal framework is robust and has not been breached and that no further information can be provided to the public - lack credibility and will do nothing to restore public confidence, given the gravity of the claims.

While we fully accept that the UK government has a duty to protect national security and prevent crime, there is an important distinction

between taking steps that are necessary and proportionate to achieve those aims and monitoring indiscriminately the communications of millions of people in the UK and other countries who are under no suspicion whatsoever.

As you know, under the European Convention on Human Rights (ECHR), and the Human Rights Act (HRA) which incorporates it into domestic law, the UK must respect the right to private life and any interference with this right must be “in accordance with the law” and “necessary in a democratic society”, and it must be proportionate.

It is hard to reconcile these principles and legal duties with what is reported about the actions of GCHQ. If the reported allegations are true, the right to privacy of millions of people in and outside the UK has been breached. To date, the government has not presented information that satisfactorily disproves the claims.

There are five specific areas where Human Rights Watch believes that clarification of UK government policy is essential.

Firstly, can you confirm or deny whether it is the case that the communications and data pertaining to millions of people in the UK have been intercepted and collected by GCHQ and can you explain the compatibility of this action with the UK’s national and international human rights obligations to uphold the right to privacy?

Secondly, can you explain how the UK government interprets the powers given to security and intelligence agencies under the Regulation of Investigatory Powers Act 2000 (RIPA)? Our understanding is that these powers allow a senior government minister to issue a warrant at the request of a senior intelligence or police official that authorises the interception of communications, where the sender or intended recipient is in the UK, if he or she believes such a warrant is necessary and proportionate. It seems that the grounds for granting a warrant under the law are extremely broad. In addition to permitting a warrant if it is “necessary” in the interests of national security, the law also permits a warrant if it is “necessary” for preventing or detecting serious crime or safeguarding the economic well-being of the UK.

The RIPA further allows a senior government minister to issue a certificate that allows a warrant to be granted for interception of communications sent or received outside the “British Isles”, without specifying a named person or premises. Given that a significant proportion of internet traffic, including by people in the UK, is routed abroad, could you explain whether and how the UK government has interpreted powers granted by RIPA to justify such indiscriminate interception of communications and data through fibre-optic cables? Once the interception has taken place, what is the process by which data is selected for use? Are there any efforts to exclude data relating to people living in the UK and if so, on what legal basis and according to what criteria? What safeguards, if any, exist on the processing, retention or sharing of such data with third parties?

Thirdly, can you confirm whether it is the case that GCHQ has been intercepting and collecting data on the citizens of other countries and the legal basis or constraints under which this action is undertaken? What safeguards, if any, exist that limit how intelligence agencies may use, retain or share such data with third parties? As you know, the German Justice Minister has

written to the UK government asking to what extent the GCHQ programme has targeted German citizens, but we pose the question as it relates to other citizens, too.

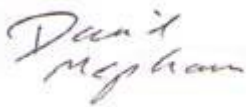
Fourthly, have intelligence agencies shared intercepted data with the NSA or any other government? If so, how much data is shared and on what legal basis? Does GCHQ request or receive data intercepted by the NSA or other governments related to persons located in the UK without a warrant?

Fifthly, in the light of these reports, do you believe that the existing oversight and accountability mechanisms in this area are adequate to prevent abuse of surveillance powers, and are consistent with the UK's human rights obligations? Human Rights Watch believes they are not. While the law provides that an Interception of Communications Commissioner can oversee the government's power to authorise interceptions, the Commissioner is appointed by the Prime Minister and reports directly to him. He retrospectively examines a number of interception warrants and assesses whether they comply with the criteria of necessity and proportionality. But it is not clear how many cases he looks at and the contents of his published annual report must be approved by the Prime Minister.

In the thirteen years since the UK's new law on intercepting communications was introduced, technology has obviously evolved very dramatically. Recent reports are highly disturbing and we urge an urgent clarification of UK government policy in this area, in response to the questions posed above. But we also favour a wider reassessment of the legal framework that applies to these issues. To ensure that the right to privacy is upheld and that the law is brought up to date, we suggest that the UK government needs to undertake a comprehensive review of the legal framework and oversight mechanisms relating to the interception of personal data and communications.

We are also very worried about the wider international implications and what this will mean for the ability of the Foreign & Commonwealth Office and the UK government to speak up for internet freedom around the world. The UK government has been a leading member of the Freedom Online Coalition, a group of governments that have made strong public commitments to protecting human rights online. Without decisive action by the UK government to clarify the strict limits and legal underpinning of any surveillance activity, the UK will not carry credibility on these issues with others. This is another reason why clarity about the UK position and a comprehensive overhaul of the relevant legal framework are essential.

Yours sincerely,

A handwritten signature in dark ink, appearing to read "David Mepham". The signature is written in a cursive, slightly slanted style.

David Mepham
UK Director
Human Rights Watch