

Obama's War on the Internet

By Philip Giraldi

[View all 25 articles by Philip Giraldi](#)

Published 07/19/10



SUBSCRIBE

[Printer-](#)

[friendly version](#)

The Ministry of Truth

The Ministry of Truth was how George Orwell described the mechanism used by government to control information in his seminal novel 1984. A recent trip to Europe has convinced me that the governments of the world have been rocked by the power of the internet and are seeking to gain control of it so that they will have a virtual monopoly on information that the public is able to access. In Italy, Germany, and Britain the anonymous internet that most Americans are still familiar with is slowly being modified. If one goes into an internet café it is now legally required in most countries in the European Union to present a government issued form of identification. When I used an internet connection at a Venice hotel, my passport was demanded as a precondition and the inner page, containing all my personal information, was scanned and a copy made for the Ministry of the Interior -- which controls the police force. The copy is retained and linked to the transaction. For home computers, the IP address of the service used is similarly recorded for identification purposes. All records of each and every internet usage, to include credit information and keystrokes that register everything that is written or sent, is accessible to the government authorities on demand, not through the action of a court or an independent authority. That means that there is de facto no right to privacy and a government bureaucrat decides what can and cannot be "reviewed" by the



Philip M. Giraldi is a former CIA counter-terrorism specialist and military intelligence officer who served 19 years overseas in Turkey, Italy, Germany, and Spain. He was Chief of Base in Barcelona from 1989 to 1992, was designated as senior Agency officer for support at the Olympic Games, and served as official liaison to the Spanish Security and Intelligence services. He has been designated by the General Accountability Office as an expert on the impact of illegal immigration on

authorities. Currently, the records are maintained for a period of six months but there is a drive to make the retention period even longer.

The excuses being given for the increasing government intervention into the internet are essentially two: first, that the anonymity of the internet has permitted criminal behavior, fraud, pornography, and libel. Second is the security argument, that managing the internet is an integral part of the "global war on terror" in that it is used by terrorists to plan their attacks requiring governments to control those who use it. The United States government takes the latter argument one step farther, claiming that the internet itself is a vulnerable "natural asset" that could be seized or damaged by terrorists and must be protected, making the case for a massive \$100 billion program of cyberwarfare. Senator Joseph Lieberman (D-CT) argues that "violent Islamist extremists" rely on the internet to communicate and recruit and he has introduced a bill in the Senate that will empower the president to "kill" the internet in case of a national emergency.

But all of the arguments for intervention are essentially themselves fraudulent and are in reality being exploited by those who favor big government and state control. The anonymity and low cost nature of the internet means that it can be used to express views that are unpopular or unconventional, which is its strength. It is sometimes used for criminal behavior because it is a mechanism, not because there is something intrinsic in it that makes it a choice of wrongdoers. Before it existed, fraud was carried out through the postal service and over the telephone. Pornography circulated freely by other means. As for the security argument, the tiny number of actual terrorists who use the internet do so because it is there and it is accessible. If it did not exist, they would find other

terrorism.

Phil Giraldi is now the Francis Walsingham Fellow at The American Conservative Defense Alliance and provides security consulting for a number of Fortune 500 corporate clients. As a counter-terrorism expert, he has assisted multinational corporations in the upgrade of their security at overseas sites to help them comply with the Patriot Act. He was one of the first American civilians to travel to Afghanistan after the fall of the Taliban, was brought in for consultation by the Port Authority of the City of New York in its planning, has assisted the United Nations security organization, and has helped

ways to communicate, just as they did in pre-internet days. In fact, intelligence sources report that internet use by terrorists is rare because of persistent government monitoring of the websites.

The real reason for controlling the internet is to restrict access to information, something every government seeks to do. If the American Departments of Defense and Homeland Security and Senator Lieberman have their way, new cybersecurity laws will enable Obama's administration to take control of the internet in the event of a national crisis. How that national crisis might be defined would be up to the White House but there have been some precedents that suggest that the response would hardly be respectful of the Bill of Rights. Many countries already monitor and censor the internet on a regular basis, forbidding access to numerous sites that they consider to be subversive or immoral. During recent unrest, the governments of both Iran and China effectively shut down the internet by taking control of or blocking servers. Combined with switching off of cell phone transmitters, the steps proved effective in isolating dissidents. Could it happen here? Undoubtedly. Once the laws are in place a terrorist incident or something that could be plausibly described in those terms would be all that is needed to have government officials issue the order to bring the internet to a halt.

But the ability to control the internet technically is only part of the story. Laws are being passed that criminalize expressing one's views on the internet, including both "hate crime" legislation and broadly drafted laws that make it a crime to support what the government describes loosely as terrorism in any way shape or form. Regular extra-legal government intrusion in the private lives of citizens is already a reality, particularly in the so-called Western Democracies that have the necessary technology and tech-savvy manpower to tap phones and invade computers. In Europe, draconian anti-terrorism laws enable security agencies to

develop a security training program for the United States Merchant Marine. He has written op-ed pieces for the Hearst Newspaper chain, is a columnist for AntiWar.com, and a contributing editor to American Conservative magazine. His media appearances include Good Morning America, MSNBC, NPR, BBC, FOX News, Polish National Television, al-Jazeera, and 60 Minutes. Phil was awarded an MA and PhD from the University of London in European, and speaks Spanish, Italian, German, and Turkish.

monitor phone calls and e-mails, in many cases without any judicial oversight. In Britain, the monitoring includes access to detailed internet records that are available for inspection by no less than 653 government agencies, most of which have nothing whatsoever to do with security or intelligence, all without any judicial review. In the United States, the Pentagon recently sought an internet and news "instant response capability" which it dubbed the Office of Strategic Influence and it has also seeded a number of retired military analysts into the major news networks to provide a pro-government slant on the war news. The State Department is also in the game, tasking young officers to engage presumed radicals in debate on their websites while the growing use of national security letters means that private communications sent through the internet can be accessed by Federal law enforcement agencies. The Patriot Act created national security letter does not require judicial oversight. More than 35,000 were issued by the FBI last year and the recipient of a letter commits a felony if he or she reveals the receipt of the document. In a recent case involving an internet provider in Philadelphia, a national security letter demanded all details of internet messages sent on a certain date, to include account information on clients with social security numbers and credit card references.

The danger is real. Most Americans who are critical of the actions of their own government rely on the internet for information that is uncensored and often provocative, including sites like Campaign for Liberty. As this article was being written, a story broke reporting that Wordpress host Blogetery had been shut down by United States authorities along with all 73,000 Blogetery-hosted blogs. The company's ISP is claiming that it had to terminate Blogetery's account immediately after being ordered to do so by law enforcement officials "due to material hosted on the server." The extreme response implies a possible presumed terrorist connection, but it is important to note that no one was charged with any actual offense, revealing that the government can close down sites based only on suspicion. It is also likely only a matter of time before Obama's internet warfare teams surface either at the Defense Department or at State. Deliberately overloading and attacking the internet to damage its credibility, witness the numerous sites that have been "hacked" and have had to cease or restrict their activities. But the moves afoot to create a legal framework to completely shut the internet down and thereby control the "message" are far more dangerous. American citizens who are concerned about maintaining their few remaining liberties should sound the alarm and tell the politicians that we don't need more government abridgement of our First Amendment rights.

Copyright © 2010 Campaign for Liberty

Also by Philip Giraldi:

[A Tea Party to Nowhere](#) 06/03/10

[Droning On](#) 05/11/10

[Change at CIA?](#) 04/22/10

[No Special Relationships](#) 04/02/10

[David Ignatius/Neo-Con Media: Oh What a Lovely War](#) 03/06/10

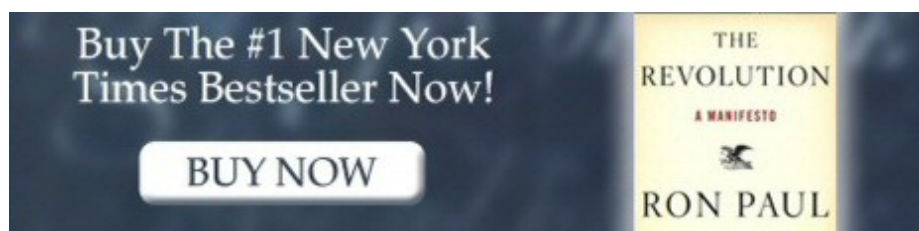
[View all 25 articles by Philip Giraldi](#)

[Discuss this article](#) (9 comments)



"Educate and inform the whole mass of the people... They are the only sure reliance for the preservation of our liberty."

—Thomas Jefferson



Campaign for Liberty is a 501(c)4 lobbying organization which neither supports nor opposes candidates for public office and claims no responsibility for the actions of individuals or groups of individuals who use the Campaign for Liberty logo or name or who may claim to act as representatives of the Campaign for Liberty without prior written consent of the Campaign for Liberty. [2]

© 2010 Campaign For Liberty | 5211 Port Royal Road, Suite 310, Springfield, VA 22151 | (703) 865-7162 (V) | (703) 865-7549 (F) | [Content standards](#)