Orwell Would Be Shocked: UK Demands Total State Snooping Rights

by Daniel Platt

March 4—Government attempts to spy on and control the use of the internet for the discussion of political ideas have reached a new and yet more dangerous phase. In the vanguard of this ominous trend is the United Kingdom.

According to an article published February 7 in the *Washington Post*, a secret order was issued earlier this year by the British government, regarding encrypted material stored on the internet. The paper cited anonymous sources, including a "former White House security adviser," who confirmed the existence of the order. According to the *Post*, "The British government's undisclosed order, issued last month, requires blanket capability to view fully encrypted material, not merely assistance in cracking a specific account, and has no known precedent in major democracies." Presumably, the *Post* includes the United Kingdom among what it calls "major democracies."

How Does Encryption Work?

Many internet messaging apps, including Signal, WhatsApp and Messenger, offer what is called "end-to-end encryption," which means that messages sent with these services are protected from peeping by anyone other than the sender and the recipient. The companies themselves are ostensibly unable to eavesdrop on encrypted communications. However, as soon as a message is backed up in "the cloud," it becomes fair game for surveillance, and internet companies have become increasingly aggressive about pushing customers to use their cloud services.

The one exception to the practice of cloud snooping is Apple, which for several years has offered a service called "Advanced Data Protection," which is encrypted cloud storage that can only be accessed by the customer. This has become a particular bone of contention for the British government, which has demanded that Apple create a "back door" which would grant it access to encrypted material stored by user accounts not only in the UK, but *anywhere in the world*.

The Surveillance State

Following the September 11, 2001 attacks, neocons exploited the public's trauma to introduce remarkably broad surveillance measures, such as the infamous Patriot Act, which gave law enforcement agencies broad authority to wiretap both domestic and foreign phone conversations, and allowed internet service providers (ISPs) to disclose customer records voluntarily to the government in emergencies. We have subsequently seen that ISPs have been willing to "voluntarily" disclose all sorts of things to government agencies, and should an ISP prove reluctant, those agencies also have the option of getting a search warrant from the Foreign Intelligence Surveillance Act (FISA) Court, which Director of National Intelligence Tulsi Gabbard at one point described as "a dependable rubber stamp for government requests." In addition to the spying, the companies have shown a remarkably cooperative


PUBLIC LAW 107-56

H. R. 3162

One Hundred Seventh Congress
of the
United States of America

AT THE FIRST SESSION

Begun and held at the City of Washington on Wednesday, the third day of January, two thousand and one

An Act

To deter and punish terrorist acts in the United States and around the world, to enhance law enforcement investigatory tools, and for other purposes.

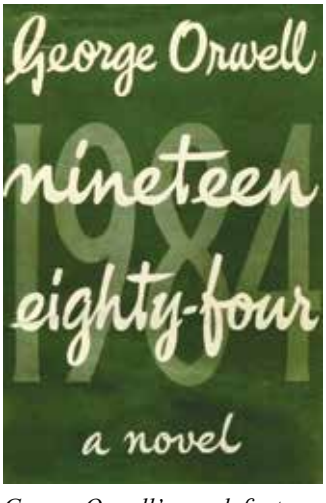
Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE AND TABLE OF CONTENTS.

Legislation for the U.S. Patriot Act.

spirit with regard to the control and suppression of political speech, to the point where, throughout 2020, the FBI was essentially supervising Twitter's censorship policy (see "The Liars' Bureau," *EIR*, January 24, 2025).

However, for many of these companies, the demands by the British regime that it be given unfettered, global access to the digital activities of the world's population constitute a bridge too far. Apple has been served with a document called a Technical Capability Notice, ordering it to provide access under the sweeping UK Investigatory Powers Act of 2016, a law which actually makes it a criminal offense to reveal to a targeted person that the government is seeking their private data, or that their promised safeguards against cloud snooping were no longer in effect. Apple, in response, is threatening to cease offering its cloud backup services in the UK, although that still leaves open the question of British demands for access to accounts *worldwide*. The president of Signal said, "Using Technical Capability Notices to weaken encryption around the globe is a shocking move that will position the UK as a tech pariah, rather than a tech leader. If implemented, the directive will create a dangerous cybersecurity vulnerability in the nervous system of our global economy."



George Orwell's novel, first edition, 1949.

The British Lead the Way

George Orwell was the British author who presciently warned in his 1949 novel *1984* of his government's trajectory toward authoritarian lust for control of political speech, and ultimately, political thought. He could not have foreseen the fabulous array of technical options available to modern-day secret policemen, particularly after the advent of the internet. But he did anticipate some of the linguistic innovations (called "newspeak" and "thoughtcrime" in the novel), such as the extremely flexible definition of "hate speech" which was used under the Terrorism Act 2000 to arrest


TLO

Mike Robinson, co-editor of the UK Column, on the Feb. 2 webcast of The LaRouche Organization.

Haim Bresheeth, a child of Holocaust survivors and the founder of the Jewish Network for Palestine, after he spoke at a demonstration in November of 2024 and accused Israel of genocide.

A similar rationale was used in the persecution of well-known journalists Richard Medhurst, who was seized at London's Heathrow Airport on August 15 last year and held for almost 24 hours as all his electronic devices and journalistic equipment were confiscated; and Kit Klarenberg, who had experienced a similar


Richard Medhurst Facebook page

British independent journalist of Syrian origin, Richard Medhurst.

ambush at London's Luton Airport in May of 2023.

On February 8 of this year, UK activist Mike Robinson appeared on the weekly "Manhattan Project" video program of The LaRouche Organization, where he presented an overview of the British government's demand for access to private data, and for broad powers to regulate what will be considered acceptable political speech.

> It comes from a piece of legislation called the Investigatory Powers (Amendment) Act 2024. This amends legislation called RIPA, the Regulation of Investigatory Powers Act, which has been around for a lot of years. But it takes state snooping in the UK to an unprecedented level.
>
> Let's just have a look at what is in it. In the Amendment, which is now in legislation—in force—the government has decided to reduce already weak protections against security services using our data illegally. This is something RIPA was designed to address. Security services were illegally snooping on people, and the original RIPA legislation was designed to retrospectively make that legal; and this goes even further. The government has removed what they call a "reasonable expectation of privacy." The government has now explained why the reduction of privacy is necessary rather than "convenient." It potentially permits bulk data collection of facial images and social media data. It absolutely permits bulk collection of internet connection data; in fact, it's a legal requirement for internet service providers in the UK to collect metadata on what websites people are looking at, and how long they're spending there and these kinds of things. It expands the range of politicians who can authorize the surveillance of other politicians; so this is not just about the state surveilling members of the public, it's also the state surveilling other politicians. You've got to ask, are they really that scared about the situation at the moment?
>
> It requires the tech companies to inform the government of any plans to strengthen security or privacy features in their software. It permits government vetoing of such security or privacy features. Anything any company wants to do to improve the security for their users, the UK government can say no to that if they want that software or that service to be available in the United Kingdom….
>
> This legislation can't be taken on its own, of course, because it needs to be looked at in combination with, for example, the Online Safety Act, which I've spoken about many times before. It effectively outlaws end-to-end encryption here in the UK in combination with the Online Safety Act. And it actually puts the West in a very interesting position, because with Trump demanding an end to state-sanctioned corporate censorship, the UK and the European Union seem to be doubling down on it….
>
> Secondary to this, I just wanted to let you know the latest developments on the Online Safety Act, as well, in this censorship regime in this country, because what's going on in the United States is very different, as we have seen over the last couple of weeks. But here now, the UK government is determined that anybody who is providing any kind of service for user-to-user chat as they discuss, or user-to-user communications, no matter how big or small, is going to have to be a proxy for the state….
>
> They claim these requirements have been put in place to prevent illegal content from being posted online. But the first problem here is that the definition of illegal content—particularly with respect, for example, to the definition of hate speech—is completely arbitrary. A perfect example of that is Richard Medhurst, who we've spoken about on this program before, who is posting content in support of Palestine which was perceived by the UK state to be supportive of a proscribed organization—in this case, Hamas. So, we have seen the definition of hate speech being redefined in recent years. Therefore, the definition of what is illegal content on the internet is being redefined on a regular basis.

Response from U.S. Officials

In the week that followed the Manhattan Project broadcast, Oregon Senator Ron Wyden (D) and Arizona Congressman Andy Biggs (R) made public a letter written to Director of National Intelligence Tulsi Gabbard, in which they write:

> We write to urge you to act decisively to protect the security of Americans' communica-

Tulsi Gabbard webpage

Director of National Intelligence Tulsi Gabbard at the U.S.-Mexican border, March 5.

> tions from dangerous, shortsighted efforts by the United Kingdom (UK) that will undermine Americans' privacy rights and expose them to espionage by China, Russia and other adversaries….
>
> While the UK has been a trusted ally, the U.S. government must not permit what is effectively a foreign cyberattack waged through political means. If the UK does not immediately reverse this dangerous effort, we urge you to re-evaluate U.S.-UK cybersecurity arrangements and programs as well as U.S. intelligence sharing with the UK….

Although the letter does genuflect to the neocons by framing the issue in the context of a hypothetical threat from Russia and China, and warning darkly of "PRC-affiliated hackers," it does nonetheless represent a highly unusual challenge to the sanctity of the U.S. "special relationship" with the UK. The two elected officials also announced a draft of the Global Trust in American Online Services Act, which Wyden says will "fix the loopholes in the CLOUD Act":

> The CLOUD Act, enacted in 2018, enables foreign countries to obtain data directly from U.S. firms, bypassing the U.S. legal system once they enter into an agreement with the Justice Department. However, the CLOUD Act failed to require foreign countries to adopt the same due process requirements long guaranteed under U.S. law, enabling foreign governments to demand that U.S. technology companies weaken the security of products used by Americans and putting global trust in U.S. firms at risk.

Whether "due process requirements long guaranteed under U.S. law" are presently taken seriously by American police agencies is subject to debate. However, there seems to be no doubt that they are treated with contempt in the UK.

In response to the Wyden-Biggs letter, Gabbard wrote:

> I was not made aware of this reported order, either by the United Kingdom government or Apple, prior to it being reported in the media. I have requested my counterparts at CIA, DIA, DHS, FBI and NSA to provide insights regarding the publicly reported actions, and will subsequently engage with UK government officials. The UK's Investigatory Powers Act of 2016, also known as the Snoopers' Charter, which I understand would be at issue, allows the UK to issue a "gag order," which would prevent Apple or any company from voicing their concerns with myself, or the public. I have directed a senior Intelligence Community officer to work with ODNI's Office of Civil Liberties, Privacy, and Transparency and ODNI's Office of Partner Engagement, to outline the potential implications of the United Kingdom compelling an American company to create a "back door" that would allow the UK government to retrieve private user content….
>
> Any information sharing between a government—any government—and private companies must be done in a manner that respects and protects the U.S. law and the Constitutional rights of U.S. citizens….

American citizens who demanded that their elected officials confirm Gabbard as DNI will soon learn whether she is prepared to go to the mat with the slobbering Anglophiles of the neoconservative movement, who have done such damage to both our national security, and to political freedom in the United States.