Governments escalate the global war on online anonymity

Stephen Parker
24 May 2026

Four months ago, the *World Socialist Web Site* analyzed the coordinated international offensive to abolish online anonymity and impose universal systems of digital identification under the cynical pretext of "child safety." Since that report, the assault has entered a far more dangerous stage, spreading across every pillar of online life.

What is unfolding is not a collection of disconnected regulatory disputes or well-meaning policy overreach. It is a coordinated offensive by the ruling classes of the major imperialist powers—the United States, the European Union, the United Kingdom, Canada and Australia—against the democratic rights of the working class. The objective is a permanent, identity-verified system of mass surveillance in which every act of communication, association and political expression is tethered to a state-issued identity record, visible to governments, corporations and employers in real time.

The dangers that online platforms pose to young people are real, and socialists are not indifferent to them. AI chatbots that have coached children toward suicide, the documented links between excessive social media usage and a deepening mental health crisis among youth, the predatory data-harvesting business models of the technology giants—these are genuine social problems, the bitter fruit of the subordination of technology to private profit.

But the governments now invoking these dangers are the same ones arming the Israeli military's slaughter of children in Gaza, gutting school funding, dismantling child welfare programs and conscripting youth for imperialist wars. Their supposed concern for the wellbeing of minors is a fraud. The real target is the independent political organization of the working class, which the ruling class is desperate to suppress before it can develop outside official control. Since 2011, from the Arab Spring to the Yellow Vests and the mass movement against the Gaza genocide, encrypted communication and online anonymity have proven indispensable tools of class struggle, and it is precisely this capacity that the surveillance drive aims to destroy.

The "child safety" Trojan horse

The most direct expression of this agenda in the United States is the GUARD Act, which the Senate Judiciary Committee advanced on April 30, 2026, in a unanimous 22-0 vote. The bill, sponsored by fascist Republican Senator Josh Hawley with bipartisan support, would require every American user of an AI chatbot—including search assistants, homework helpers and customer service systems—to upload a government-issued identification document, submit a facial scan or provide financial records before being permitted to interact with the system.

Presented as a measure to stop AI platforms from encouraging self-harm among the young, it would in practice establish a universal national identity check for the entire digital sphere, with criminal penalties of up to 20 years imprisonment for providers whose systems solicit sexual content or self-harm from minors.

The committee's unanimous vote reflects the consensus of the American ruling class that online anonymity must be abolished. There is no meaningful wing of the political establishment, Democratic or Republican, that opposes the principle of identity verification as a precondition for digital participation.

At the state level, Pennsylvania's Democratic Governor Josh Shapiro, leveraging a lawsuit against an AI company following the suicide of a teenager, has proposed what amounts to an "ID-to-chat" regime. His plan would require digital identification before conversations could take place and mandate that companies scan every message sent by a minor, with "flagged" content automatically reported to law enforcement without human review. Algorithmic filters cannot grasp the nuances of human speech; they are blunt instruments designed not to protect vulnerable young people but to place an entire generation under permanent monitoring.

Australia's under-16 social media ban, which took effect in late 2025 and was analyzed by the *World Socialist Web Site*, has now produced concrete results that expose its fraudulent character. A study from the University of Chicago's Becker Friedman Institute found that 73 percent of targeted teenagers are simply ignoring it, with compliance highest among isolated, "less popular" youth—precisely those the legislation claimed to protect. The social environment it was ostensibly designed to transform is unchanged.

What has changed is the normalized testing, on a captive population, of age-estimation algorithms, behavioral inference systems and facial-scanning technologies. The platforms face fines of up to $49.5 million (AUD) for non-compliance, a powerful incentive to become arms of state monitoring. As we noted last December, the real aim of the ban is to suppress growing opposition among young people to war, austerity and dictatorship and prevent it from finding organized political expression.

The European Union's regulatory dictatorship

The European Commission, under Executive Vice-President Henna Virkkunen, has emerged as perhaps the most aggressive institutional actor in the global crackdown. Under the Digital Services Act (DSA), Brussels has provisionally concluded that Meta, the parent company of Facebook and Instagram, failed to adequately prevent children under the age of 13 from accessing its platforms. The Commission is now threatening fines of up to 6 percent of Meta's global annual turnover, a figure that could exceed $12 billion, unless the company implements rigorous identity verification for all users.

The choice now being imposed on every social media platform operating in Europe is explicit: maintain a behavioral surveillance file on every user or demand a government-verified identity document from each one. No third option exists. This is a direct strike at the ability of dissidents, whistleblowers, journalists and political organizers to communicate without being permanently tethered to a state-issued record.

More significant still is Brussels' targeting of the tools workers use to protect themselves from surveillance. A European Parliamentary Research Service briefing has openly labeled virtual private networks (VPNs) a "loophole" that must be closed, and Executive Vice-President Henna Virkkunen has signaled that preventing VPN circumvention of verification systems is a core priority for the EU's "next steps." The irony is that the Commission made this declaration even as its own model "age verification app," promoted as a blueprint for bloc-wide implementation, was broken by security researchers within minutes of its source code being made public.

The war on encryption: From Canada to France

Perhaps the most alarming development of recent months is the intensified assault on end-to-end encryption, the mathematical foundation of private communication in the digital age.

In Canada, the Liberal government's Bill C-22, marketed as a "Lawful Access" measure, would compel telecommunications and internet companies to rebuild their technical infrastructure to provide permanent state access to communications. The bill would require providers to retain metadata on every subscriber for up to a year, creating a comprehensive map of the entire population's movements, associations and communications.

When cybersecurity experts, civil society organizations and companies including Apple and Signal raised the alarm—Signal threatening to withdraw from the Canadian market rather than compromise its privacy architecture—government officials dismissed the critics as people who "don't understand" the legislation.

The government's defense is itself the most damning indictment of its intent: It insists that building a backdoor does not "interrupt" encryption. Every working cryptographer knows this is false. A backdoor accessible to "the good guys" is a backdoor accessible to everyone, as was demonstrated in practice by the Salt Typhoon hack, in which foreign actors penetrated US law enforcement's own wiretapping access systems.

The Canadian House of Commons has, separately, begun maintaining a database of social media posts deemed "misogynistic" or "abusive" toward members of parliament, a chilling model for state-directed political surveillance dressed up as a defense of legislators' personal dignity.

In France, parliament's intelligence delegation has formally backed a "ghost participant" proposal that would require messaging platforms such as WhatsApp and Signal to silently add an invisible state agent to supposedly private encrypted conversations. Its architects call this a compromise. It is in fact a total capitulation to the police and intelligence services, which have spent years arguing that mathematical privacy "hinders" their work. If enacted, no private conversation conducted on a digital platform could be presumed secure in France—and given how such platforms operate globally, a French backdoor is effectively a backdoor for the world.

The end of anonymous speech and assembly

In the United Kingdom, the mask of democratic tolerance has been removed entirely. Ofcom, Britain's speech regulator, has asserted the right to exercise what can only be described as global speech control. It recently fined an American mental health forum nearly £1 million for content hosted on American servers, despite the site having already geoblocked British visitors. Ofcom's stated logic, that a website is "accessible" in Britain if a user employs a VPN to circumvent a geographic block, renders every website on earth theoretically liable to British jurisdiction.

The capitulation of Elon Musk's X to Ofcom is particularly revealing. After publicly attacking the UK's Online Safety Act as dangerous overreach, X has now agreed to a 48-hour content removal pipeline, with compliance audited by organizations such as the Centre for Countering Digital Hate, a group with a documented record of targeting legitimate political speech. This is the trajectory of all nominally "anti-censorship" platforms operating within the framework of capitalism: However loudly their proprietors rail against regulation, they remain subject to the same market and legal pressures that drive their competitors to censor.

As the *World Socialist Web Site* has documented extensively, the Labour government of Keir Starmer has been constructing a centralized policing apparatus explicitly designed for domestic class conflict. In January we reported on Labour's blueprint for a centralized police-state apparatus in Britain, including the £140 million commitment to deploy 40 additional Live Facial Recognition (LFR) vans across England and Wales. The white paper's technical program, revealed in that report, has now been operationalized.

For the first time in British history, the Metropolitan Police deployed live facial recognition technology at a political protest, scanning the faces of attendees at the "Unite the Kingdom" rally in Camden. By operationalizing fleets of mobile LFR vans at street demonstrations alongside parallel pilot programs featuring fixed cameras permanently bolted to lamp posts, the Metropolitan Police is constructing a biometric record of political participation that did not require a single parliamentary vote to authorize. That protesters now know they are being scanned and catalogued is itself the political objective: The chilling effect on assembly is the very mechanism of social control.

Nearly 4.7 million faces were scanned by British police using live facial recognition in the year to May 2025, more than double the figure recorded the previous year. The advocacy group Big Brother Watch has described this rapid expansion as "one of the most significant threats to civil liberties in the history of British policing," while the Liberty advocacy group has warned that the technology entrenches structural bias against working-class and minority communities. The Starmer government is responding by institutionalizing and expanding it.

In the United States, the Federal Communications Commission (FCC) has proposed ending anonymous prepaid mobile phone service by requiring government identification for all SIM card purchases. For domestic violence survivors, whistleblowers, journalists with sensitive sources and political organizers, prepaid phones are one of the last remaining means of separating their communications from their legal identity. The FCC proposal would close it entirely.

The TAKE IT DOWN Act, passed with bipartisan support, creates a broad censorship mechanism lacking the procedural safeguards even the most limited democratic system would normally demand. Congress also quietly extended the National Security Agency's Section 702 warrantless surveillance authority for a further 45 days, without the congressional debate the issue demands—a measure of how normalized the wholesale violation of Fourth Amendment protections has become across both parties of the capitalist establishment.

The logic of coordinated repression

The convergence of these measures across so many jurisdictions is not accidental. The ruling class of each major imperialist country has reached the same conclusion independently, because each confronts the same reality: a program of war, austerity and social reaction that cannot be implemented through genuinely democratic means.

The international working class has demonstrated, through strikes and mass protests against genocide organized via encrypted communications outside the control of the trade union bureaucracies and corporate media, that online anonymity is a material precondition for class struggle.

The same governments pursuing this agenda are conducting mass deportations, criminalizing anti-war protest, arming genocide, cutting public services to fund military budgets and preparing for expanded imperialist war.

In the United States, as we reported in February, an integrated network of surveillance, tracking and identification technologies is being deployed by ICE and CBP against immigrants and protesters, including the targeted killing of individuals identified through these systems for opposing the state.

In Britain, nearly 3,000 people have been arrested for expressing support for Palestine Action since Starmer's government proscribed the group under terrorism legislation, and the Starmer government's mass police crackdown against pro-Palestinian protesters continues to intensify.

The legislative assault on online anonymity is the digital dimension of this drive: an effort to ensure that every worker's political opinions are legible to their employer, their government and the state apparatus being prepared for class confrontation.

The technologies being tested on the stated targets—children, migrants, "extremists"—are being built for use against the entire working class. There is no historical example of a surveillance infrastructure constructed by a capitalist state that remained confined to the target group initially invoked to justify it.

The tasks of the working class

The defense of democratic rights cannot be entrusted to the courts, the capitalist parties or the technology corporations. Federal judges in the United States have blocked some state-level surveillance laws on First Amendment grounds, but the Supreme Court ruled in *Free Speech Coalition v. Paxton* (2025) that age verification is constitutionally permissible.

The European Court of Human Rights issued a ruling defending encryption in 2024, only for the EU Council to press ahead with its own surveillance framework the following year. Legal challenges within the framework of bourgeois democracy can at most slow the tempo of these attacks, not halt a drive that flows from the objective crisis of the capitalist system itself.

The working class must oppose the fraudulent "child safety" and "national security" pretexts deployed by the bourgeoisie at every turn, exposing their true character as instruments of political control. It must demand the unconditional protection of end-to-end encryption, the abolition of the surveillance state, the right to absolute anonymity in communication and online association and an end to the conscription of private technology companies into the state's monitoring apparatus.

The communications infrastructure of modern society can serve human need rather than state repression only through the expropriation of the technology monopolies and their placement under the democratic control of the working class, not through the regulation of their worst excesses.

These demands cannot be separated from the broader struggle against capitalism. The drive toward digital authoritarianism is not a policy mistake or the product of misguided legislators. It is the necessary expression of a ruling class that understands its program of permanent war and social counterrevolution cannot survive the independent political mobilization of the international working class.

The answer to that drive is the construction of precisely the kind of movement the surveillance state is being built to prevent: the international unity of workers, in the United States, Canada, Britain, France, Australia and every other country, against the capitalist system that is the ultimate source of the descent into dictatorship.