

# Twitter, WikiLeaks and the US Justice Department

Online Privacy Rights and Freedom of Expression

By [Tom Burghardt](#)

Global Research, November 13, 2011

[Antifascist Calling...](#) 13 November 2011

Region: [USA](#)

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

*In a further blow to online privacy rights and press freedom, the U.S. District Court in Alexandria, Va. ordered the microblogging site Twitter to hand over account information on three activists under investigation by the Justice Department for their links to the whistleblowing web site [WikiLeaks](#).*

Under “transparency president” Barack Obama, the U.S. government initiated a criminal probe of the organization after the site began releasing a virtual tsunami of confidential military and State Department files.

In the last two years alone, WikiLeaks revealed that the United States had committed grave war crimes in [Afghanistan](#), [Iraq](#) and other global hot-spots of interest to America’s resource-grabbing corporate masters.

This year’s release of 779 classified dossiers on prisoners housed at the [Guantánamo Bay](#) prison gulag fleshed out the public’s knowledge of ongoing torture programs run by the military and the CIA under cover of it’s murderous “War on Terror.”

But it was their publication of some 250,000 secret State Department [cables](#) which sparked a new round of hysterical denunciations in Washington culminating in the witchhunt against Julian Assange and WikiLeaks supporters, a demonization campaign aided and abetted by U.S. financial institutions such as Bank of America and Pentagon cyberwar contractors.

Cable after cable revealed “the extent of US spying on its allies and the UN; turning a blind eye to corruption and human rights abuse in ‘client states’; backroom deals with supposedly neutral countries; lobbying for US corporations; and the measures US diplomats take to advance those who have access to them.”

Leading politicians, including Vice President Joe Biden and Senate Minority leader Mitch McConnell have called the web site’s founder a “high-tech terrorist,” and commentators such as right-wing [Washington Times](#) columnist Jeffery Kuhner and others have demanded that Assange and his co-workers be treated “the same way as other high-value terrorist targets.”

The Obama administration, loathe to pursue criminal probes of the previous regime’s lawbreaking, the better to immunize themselves over their own contemporary lawless acts, including the torture of prisoners at [Bagram Airbase](#), clandestine CIA [drone killings](#) and the due process-free [assassination](#) of an American citizen who was never charged, let alone convicted of a crime, was up to the challenge and empaneled a grand jury in Alexandria, Va.

And when Justice Department inquisitors first sought to seize the activist's information, in keeping with the new "Washington consensus" that constitutional rights are nothing more than empty platitudes duly trotted out on national holidays, they demanded that Twitter turn over the files without benefit of a warrant.

American Civil Liberties Union staff attorney Aden Fine [denounced](#) the ruling. "Internet users don't automatically give up their rights to privacy and free speech when they use services like Twitter," Fine said.

"The government shouldn't be able to get this kind of private information without a warrant, and they certainly shouldn't be able to do so in secret. An open court system is a fundamental part of our democracy, and the very existence of court documents should not be hidden from the public."

According to the [ACLU](#), it wasn't only Twitter that was served with record demands by the Justice Department. "Based on the file numbers that have been created, it appears likely that there are additional orders whose existence remains secret."

The public first became aware of the government's fishing expedition only because Twitter informed the three activists, Jacob Appelbaum, a founding member of the online anonymity network, [Tor Project](#), Rop Gonggrijp, a founder of the Dutch web portal [XS4ALL](#) and Birgitta Jónsdóttir, a left-wing member of Iceland's Parliament.

As [Antifascist Calling](#) reported in March, Jónsdóttir was specifically targeted for her role in helping WikiLeaks release the [Collateral Murder](#) video last year.

That scandalous video exposed the wanton slaughter of a dozen people in the Iraqi suburb of New Baghdad, including two Reuters photojournalists, by a U.S. military Apache helicopter crew. Two children were also seriously wounded in the unprovoked attack.

The Army's thrill-kill gun camera video wasn't concealed from the public because of any alleged threat to "national security" or to protect intelligence "sources and methods," standard boilerplate used to hide war crimes by the U.S. Empire, but precisely to *cover-up* imperialism's murderous rampage that helped "liberate" Iraqis of their lives.

Commenting on the ruling, Jónsdóttir told [The Guardian](#), "This is a huge blow for everybody that uses social media. We have to have the same civil rights online as we have offline. Imagine if the US authorities wanted to do a house search at my home, go through my private papers. There would be a hell of a fight. It's absolutely unacceptable."

Unfortunately, under [Section 213](#) of the oxymoronic USA Patriot Act, which was not subject to a "sunset" provision of the constitution-shredding legislation, FBI agents can do precisely that and obtain so-called "delayed notification" warrants for the search and seizure of evidence of any federal crime, not only those related to "terrorism" investigations.

Called "sneak and peek" searches, federal snoops are permitted to clandestinely seize property or conduct electronic searches on a home computer if a court deems such seizures "reasonably necessary." Indeed, notification of a covert FBI home invasion "may thereafter be extended by the court for good cause shown."

The sweeping ruling by Judge Liam O'Grady upheld demands by U.S. investigators that they

should have virtual free-reign to pillage private records related to the users' IP address, the unique identifier used by a computer or hand-held device to log onto the internet.

According to the Electronic Frontier Foundation ([EFF](#)) who represent Jónsdóttir along with American Civil Liberties Union attorneys, O'Grady "also blocked the users' attempt to discover whether other Internet companies have been ordered to turn their data over to the government."

"When you use the Internet, you entrust your online conversations, thoughts, experiences, locations, photos, and more to dozens of companies who host or transfer your data," EFF Legal Director Cindy Cohn said.

"In light of that technological reality, we are gravely worried by the court's conclusion that records about you that are collected by Internet services like Twitter, Facebook, Skype and Google are fair game for warrantless searches by the government."

Among other things, O'Grady wrote in his 60-page [decision](#) that "the information sought was clearly material to establishing key facts related to an ongoing investigation and would have assisted a grand jury in conducting an inquiry into the particular matters under investigation."

O'Grady, appointed to the United States District Court for the Eastern District of Virginia in 2007 by President George W. Bush, argued that because Twitter users "voluntarily" turned over their IP addresses when they signed up for an account, they lost any expectation of privacy.

In other words, simply because users click through opaque "Terms of Service" agreements with Twitter, Google, Facebook or any other internet vendor, "petitioners knew or should have known that their I.P. information was subject to examination by Twitter, so they had a lessened expectation of privacy in that information, particularly in light of their apparent consent to the Twitter terms of service and privacy policy."

However, as security researcher Christopher Soghoian pointed out in [Slight Paranoia](#), "The federal judge in the Wikileaks case cited in his order a version of Twitter's privacy policy from 2010, rather than the very different policy that existed when Appelbaum, Gonggrijp and Jonsdottir created their Twitter accounts back in 2008."

"That older policy," Soghoian wrote, "actually promised users that Twitter would keep their data private unless they violated the company's terms of service. It is unclear how the judge managed to miss this important detail."

"There is a slight problem with relying on a privacy policy created on November 16, 2010 to decide the reasonable expectation of privacy of these three individuals: They created their Twitter accounts several years before the document was written."

Indeed, as Soghoian observes, "not only is a federal judge ruling that 3 individuals have no reasonable expectation of privacy with regard to the government getting some of their Internet transaction data, but the judge isn't even citing the right version of a widely ignored privacy policy to do so."

"If the judge were to examine the privacy policy that existed when these three targets signed up for a Twitter account," Soghoian concludes, "he might decide that they do in fact

have a reasonable expectation of privacy and that the government needs a warrant to get the data.”

While true as far as it goes, and Soghoian should be commended for pointing out this glaring contradiction in the government’s case, readers are well aware that the WikiLeaks Twitter case is about *politics* not process, that is, moves by the secret state to clamp-down on dissent and dissenters, and not whether someone has read and “voluntarily” signed-off on a vendor’s “Terms of Service” agreement.

Among other things, O’Grady’s ruling revealed that the government was seeking not only IP addresses but “1. subscriber names, user names, screen names, or other identities; 2. mailing addresses, residential addresses, business addresses, e-mail addresses and other contact information; 3. connection records, or records of session times and durations; 4. length of service (including start date) and types of service utilized; 5. telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and 6. means and source of payment for such service (including any credit card or bank account number) and billing records.”

It doesn’t take a computer forensics expert to conclude that the government, in obtaining “connection records,” will also get their hands on information about *anyone else* who corresponded or “followed” the activists on Twitter.

Kevin Bankston, a senior staff attorney with EFF told [CNET News](#) that the ruling means that “essentially any data about you collected by an Internet service is fair game for warrantless searches by the government.”

The District Court’s ruling can be situated within the wider context of the Obama administration’s unprecedented drive to criminalize whistleblowing.

The persecution of Julian Assange and other WikiLeaks supporters is a shot across the bow not only against those who leak sensitive information to the public that expose egregious acts by the well-connected, but at investigative journalists and researchers who in their course of their work uncover high crimes and misdemeanors by powerful corporations and governments.

As the [World Socialist Web Site](#) pointed out, “Assange’s real ‘crime’ is that, through its publication of a mass of secret US military documents, diplomatic cables and video footage, WikiLeaks has exposed the criminal character of the invasions and occupations of Afghanistan and Iraq and numerous other conspiracies carried out against the world’s people by Washington and its allies.”

Make no mistake, this ruling is a warning of further draconian moves to come.

*Tom Burghardt is a researcher and activist based in the San Francisco Bay Area. In addition to publishing in Covert Action Quarterly and [Global Research](#), he is a Contributing Editor with [Cyrano’s Journal Today](#). His articles can be read on [Dissident Voice](#), [The Intelligence Daily](#), [Pacific Free Press](#), [Uncommon Thought Journal](#), and the whistleblowing website [WikiLeaks](#). He is the editor of Police State America: U.S. Military “Civil Disturbance” Planning, distributed by [AK Press](#) and has contributed to the new book from [Global Research](#), The Global Economic Crisis: The Great Depression of the XXI Century.*

The original source of this article is [Antifascist Calling...](#)  
Copyright © [Tom Burghardt](#), [Antifascist Calling...](#), 2011

---

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

[Become a Member of Global Research](#)

Articles by: [Tom Burghardt](#)  
[http://antifascist-calling.blogspot.co](http://antifascist-calling.blogspot.com/)  
[m/](#)

**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)