Department of Justice Threatens the Internet

Secret State Demands News Organization's Web Logs, Gets Slapped Down

By Tom Burghardt
Global Research, November 13, 2009
Antifascist Calling... 12 November 2009

Region: USA
Theme: Police State & Civil Rights

When the Independent Media Center (IMC) received a formal notice on January 30 from the Department of Justice, demanding they provide an Indianapolis grand jury with “details of all reader visits on a certain day,” the feisty left-wing news aggregators fought back, CBS News reported.

Investigative journalist Declan McCullagh revealed that the “change” administration’s legal eagles issued an order that required the “Philadelphia-based Indymedia.us Web site ‘not to disclose the existence of this request’ unless authorized by the Justice Department, a gag order that presents an unusual quandary for any news organization.”

Kristina Clair, IndyMedia’s Linux administrator, told CBS she was shocked to have received the subpoena with its flawed demand not to disclose its contents.

The subpoena from U.S. Attorney Tim Morrison in Indianapolis demanded “all IP traffic to and from www.indymedia.us” on June 25, 2008. It instructed Clair to “include IP addresses, times, and any other identifying information,” including e-mail addresses, physical addresses, registered accounts, and Indymedia readers’ Social Security Numbers, bank account numbers, credit card numbers, and so on. (Declan McCullagh, “Justice Dept. Asked for News Site’s Visitor Lists,” CBS News, November 10, 2009)

Talk about intrusive! While grand jury subpoenas of news organizations and journalists are not unprecedented, under long-standing guidelines these subpoenas are supposed to receive special handling given their sensitive nature, thus ensuring that even the appearance of prior restraint of a journalist’s ability to report the news is avoided.

In IndyMedia’s case however, DOJ’s ham-handed stipulation amounted to government meddling clearly prohibited by the First Amendment. Not that any of this seems to matter to an administration hell-bent on defending–and expanding–every illegal program of the previous regime.

McCullagh writes that one section of the guidelines state that “no subpoena may be issued to any member of the news media” without “the express authorization of the attorney general,” in this case, the secret state’s newest “best friend forever” Eric Holder.

Indeed, these draconian writs must be “directed at material information regarding a limited subject matter.” The government’s demand however, for virtually every piece of information held by IndyMedia on their contributors and readers hardly qualifies as “limited” even in today’s bizarro world of “national security” driftnet surveillance and data mining.

When queried by CBS as to what criminal investigation prompted their draconian demand for IP addresses "and any other identifying information" on IndyMedia users, U.S. Attorney Tim Morrison emailed CBS with a curt reply: "We Have no comment."

But before proceeding further, let's be clear on one thing: since the 1970s, the federal grand jury system where the prosecutor reigns supreme, has been an instrument wielded by the secret state to target dissent and to ensnare left-wing government critics in open-ended "investigations" whose sole purpose is to harass if not prosecute alleged "troublemakers."

As the late, great defender of civil liberties, Frank Donner, described in his landmark work on America's political intelligence system, during the lawless rampage against the left launched by the Nixon administration:

A new attack [on dissent] would have to be secret, clothed with a more plausible justification than the [red-hunting congressional] committees' claimed legislative purpose, and aimed inwardly at the group and its members.

The White House entrusted the grand jury offensive to the Internal Security Division (ISD) of the Department of Justice. This unit, which had languished during the post-McCarthy years, was now enlarged from a complement of six to sixty as part of a master plan to deploy all available resources against the new dissenters. …

The secrecy of the grand jury proceeding cloaks abuses. Although secrecy historically served to protect the independence of the grand jury by insulating it from the pressures of the Crown, there can be little doubt that in the Nixon years grand jury secrecy became an instrument of the very evil it was intended to prevent. (Frank Donner,The Age of Surveillance, New York: Alfred A. Knopf, 1980, pp. 355, 357)

Today, with antiwar groups, anarchists, socialists, animal rights and environmental activists clearly focused in the secret state's cross hairs, one can speculate that the DOJ's reticence to reveal what "crime" they were allegedly investigating in all probability related to information surreptitiously obtained by a paid informant or provocateur.

This hypothesis is all the more compelling when one considers that DOJ attorney's threatened Clair with obstruction of justice if she disclosed the existence of the subpoena, claiming it "may endanger someone's health" and would have a "human cost."

But shortly after receiving the onerous warrant Clair's shock turned to anger, and the sysadmin contacted the San Francisco-based civil liberties group, the Electronic Frontier Foundation (EFF), who agreed to take on the government.

On November 9, EFF published a whitepaper outlining the shadowy nature of the secret state's latest moves to subvert our constitutional rights. According to EFF's senior staff attorney Kevin Bankston,

Secrecy surrounds law enforcement's communications surveillance practices like a dense fog. Particularly shrouded in secrecy are government demands issued under 18 U.S.C. § 2703 of the Stored Communications Act or "SCA" that seek subscriber information or other user records from communications service providers. When the government wants such data from a phone company or online service provider, it can obtain a court order under the SCA demanding the information from the provider, along with a gag order preventing the

provider from disclosing the existence of the government's demand. More often, companies are simply served with subpoenas issued directly by prosecutors without any court involvement; these demands, too, are rarely made public. ("From EFF's Secret Files: Anatomy of a Bogus Subpoena," Electronic Frontier Foundation, November 9, 2009)

Undeterred by the quickly broken promises of the Obama regime to "restore the rule of law," like their Bushist predecessors, Obama's Justice Department is the golden shield that hides from public view the high crimes and misdemeanors of America's corporatist police state.

Readers of Antifascist Calling are urged to read EFF's well-written analysis. It meticulously dissects the lawless behavior of administration attorneys who, without skipping a beat, attempted to brow-beat a news organization into submission, thus preventing them from doing what they do best: informing the public, not as court stenographers but, as the heroic Israeli journalist Amira Hass has averred by "monitoring the centers of power."

Readers are also urged to read the government's subpoena in its entirety, an exercise in overreaching and a clear violation of the state's own guidelines governing the issuance of these onerous warrants.

Grand jury subpoenas are very easy for the government to get–they are issued directly by prosecutors without any direct court oversight. Therefore, the SCA limits what those subpoenas can obtain, in contrast to a search warrant or other court order. Under the SCA's 18 U.S.C. § 2703(c)(2), grand jury subpoenas can only be used to get basic subscriber-identifying information about a target–e.g., a particular user's name, IP address, physical address or payment details–and certain types of telephone logs; any other records require a court order or a search warrant. …

However, with the Indymedia subpoena, the government departed from the text of the law and the Justice Department's own sample subpoena by inserting this demand: "Please provide the following information pursuant to [18 U.S.C. § 2703(c)(2)]: All IP traffic to and from www.indymedia.us" for a particular date, including "IP addresses, times, and any other identifying information."

In other words, the government was asking for the IP address of every one of indymedia.us's thousands of visitors on that date–the IP address of every person who read any news story on the entire site. Not only did this request threaten every indymedia.us visitor's First Amendment right to read the news anonymously (particularly considering that the government could easily obtain the name and address associated with each IP address via subpoenas to the ISPs that control those IP blocks), it plainly violated the SCA's restrictions on what types of data the government could obtain using a subpoena. The subpoena was also patently overbroad, a clear fishing expedition: there's no way that the identity ofevery Indymedia reader of every Indymedia story was relevant to the crime being investigated by the grand jury in Indiana, whatever that crime may be. (EFF, op. cit., emphasis in original)

CBS reported that EFF wrote a series of letters to the DOJ. Thefirst detailed the flaws in the original subpoena while thesecond pointedly said that if the government needed to muzzle IndyMedia, it should apply for a formal gag order under the relevant section of federal law.

Hardly the sharpest knives in the drawer, DOJ higher-ups quickly caught on and realized that

the group was about to challenge the law on First Amendment grounds. At that point, the state backed down and withdrew the subpoena. EFF wrote, “Obviously, that was a fight–and more importantly, a precedent–that the government wanted to avoid.”

The lesson here? When the state comes knocking, the first and best line of defense is to seek competent legal advice from the relevant civil liberties’ organization.

Handing over information that the government is not legally entitled to, or indeed, answering questions posed by federal investigators trained in subtle interview techniques without an attorney present can–and has–resulted in “obstruction of justice” or a “lying to federal government agents” indictment, a crime under Title 18, United States Code, § 1001. Silence is always an option.

A good place to start learning how to fight back against electronic spying practices is a working familiarity with EFF’s excellent handbook “Surveillance Self-Defense.”

Articles by: Tom Burghardt
http://antifascist-calling.blogspot.com/