Calling Edward Snowden an 'International Human Rights Defender,' EU Resolution Calls for His Protection

Published on Thursday, October 29, 2015 by Common Dreams
by Andrea Germanos, staff writer

The European Parliament passed a resolution Thursday urging its nations to afford NSA whistleblower Edward Snowden protection.

Passed by a 285 to 281 vote, the resolution calls on EU member states to "drop any criminal charges against Edward Snowden, grant him protection and consequently prevent extradition or rendition by third parties, in recognition of his status as whistle-blower and international human rights defender."

Snowden, who's been residing in Russia since 2013, responded to the resolution on Twitter by calling it a "game-changer":

While the resolution is not binding, Wolfgang Kaleck, Snowden's lawyer in Berlin, told the*Daily Dot* in an email, "It is an overdue step and we urge the member States to act now to implement the resolution."

U.S.-based digital rights group Fight for the Future welcomed the news as well. Evan Greer, the organization's campaign director, said, "We hope that this resolution leads to a binding agreement in the EU that allows Edward Snowden to move to whichever EU country he wants, and we hope he gets an epic party thrown in his honor when he arrives."

"The battle over mass government surveillance is a decisive moment in the history of humanity, and it's hard to think of anyone who has done more than Edward Snowden to educate the

public about the grave risks that runaway spying programs pose to our basic human rights, the future of the Internet, and freedom of expression," he added.

The World Wide Web Foundation, which advocates for an open Internet and was founded by Web inventor Tim Berners-Lee, called it a "landmark resolution." It added in a statement, "We call on national leaders to publicly commit to respecting the will of the European people and offering Snowden asylum."

Berners-Lee said in a Reddit Ask Me Anything session last year that Snowden "should be protected, and we should have ways of protecting people like him. Because we can try to design perfect systems of government, and they will never be perfect, and when they fail, then the whistleblower may be all that saves society."

Filmmaker Laura Poitras Sues US Over 'Kafkaesque' Harassment

Published on Tuesday, July 14, 2015 by Common Dreams by Nadia Prupis, staff writer

Award-winning journalist and filmmaker Laura Poitras on Monday filed a lawsuit against the U.S. Department of Justice (DOJ) and U.S. intelligence agencies for subjecting her to what she called "Kafkaesque" harassment at airports throughout the U.S. and the world on dozens of occasions.

Poitras, who won an Academy Award last year for *Citizenfour*,

the documentary about NSA whistleblower Edward Snowden, said she has been detained, searched without warrant, interrogated for hours, and had vital belongings confiscated more than 50 times over the course of six years—without ever being charged with a crime.

The Freedom of Information Act (FOIA) lawsuit names the DOJ, the Department of Homeland Security, and the Office of the Director of National Intelligence and demands the release of all records from those agencies on Poitras.

In a statement on Monday, the filmmaker, who is being represented by the civil liberties group Electronic Frontier Foundation (EFF), made clear that her lawsuit stood for more than just her own experiences.

"By spurning Poitras' FOIA requests, the government leaves the impression that her detentions were a form of retaliation and harassment of a journalist whose work has focused on U.S. policy in the post-9/11 world."

—Jamie Lee Williams, Electronic Frontier Foundation

"I'm filing this lawsuit because the government uses the U.S. border to bypass the rule of law," Poitras said. "This simply should not be tolerated in a democracy. I am also filing this suit in support of the countless other less high-profile people who have also been subjected to years of Kafkaesque harassment at the borders. We have a right to know how this system works and why we are targeted."

Poitras has spoken openly about her harassment at U.S. borders, which included reportedly being placed on the government's No Fly List after returning home from filming *My Country, My Country*, a 2006 documentary which profiled Iraqi critics of the U.S. occupation.

She has also had her laptop, camera, mobile phone, and reporter notebooks seized and their contents copied, according to the suit. On one occasion, Poitras was allegedly threatened

with handcuffing for taking notes during her detention, as border agents said her pen could be used as a weapon.

This is not the first time that Poitras has filed FOIAs with intelligence agencies for their records on her detainment, but the departments have evaded her requests at every turn.

“The government used its power to detain people at airports, in the name of national security, to target a journalist whose work has focused on the effects of the U.S. war on terror,” said David Sobel, EFF senior counsel. “In refusing to respond to Poitras’ FOIA requests and wrongfully withholding the documents about her it has located, the government is flouting its responsibility to explain and defend why it subjected a law-abiding citizen—whose work has shone a light on post-9/11 military and intelligence activities—to interrogations and searches every time she entered her country.”

EFF attorney Jamie Lee Williams added: “We are suing the government to force it to disclose any records that would show why security officials targeted Poitras for six years, even though she had no criminal record and there was no indication that she posed any security risk. By spurning Poitras’ FOIA requests, the government leaves the impression that her detentions were a form of retaliation and harassment of a journalist whose work has focused on U.S. policy in the post-9/11 world.”

In addition to her documentary film work, Poitras is a recipient of the MacArthur Genius Grant and has won the Pulitzer for her reporting on the NSA leaks. *My Country, My Country*and *Citizenfour* are part of a series of films exploring post-9/11 America, along with 2010’s*The Oath*, a documentary about Guantanamo Bay prison. She also writes for *The Intercept*.

FBI Operating Mysterious Surveillance Flights in US: Investigation

Published on Tuesday, June 02, 2015 by Common Dreams by Nadia Prupis, staff writer

The U.S. Federal Bureau of Investigation (FBI) is flying small planes equipped with video and cellphone surveillance technology around the country and hiding their activities behind fictitious business fronts, the *Associated Press* revealed on Tuesday.

In its investigation, the *AP* found that the agency operated flights above more than 30 cities in 11 states, plus the District of Columbia, within a recent 30-day period—generally using surveillance equipment without a judge's approval. Some of those cities include Chicago, Minneapolis, Boston, Houston, Phoenix, Seattle, and Anaheim.

Further, the FBI used at least 13 fake companies to hide its activities, including FVX Research, KQM Aviation, NBR Aviation and PXW Services, the *AP* reports, adding, "Even basic aspects of the program are withheld from the public in censored versions of official reports from the Justice Department's inspector general."

The *AP* continues:

> *"The FBI's aviation program is not secret," spokesman Christopher Allen said in a statement. "Specific aircraft and their capabilities are protected for operational security purposes." Allen added that the FBI's planes "are not equipped, designed or used for bulk collection activities or*

> *mass surveillance."*
>
> *But the planes can capture video of unrelated criminal activity on the ground that could be handed over for prosecutions.*
>
> *Some of the aircraft can also be equipped with technology that can identify thousands of people below through the cellphones they carry, even if they're not making a call or in public.*
>
> *…Officials say cellphone surveillance is rare, although the AP found in recent weeks FBI flights orbiting large, enclosed buildings for extended periods where aerial photography would be less effective than electronic signals collection. Those included above Ronald Reagan Washington National Airport and the Mall of America in Bloomington, Minnesota.*

FBI planes have been sporadically identified in recent months, with the *Washington Post* noting two flights circling Baltimore in early May. Shortly thereafter, the Department of Justice released guidelines that explicitly barred the agency from using the aircrafts to monitor activities protected by the First Amendment, such as peaceful protests, "or the lawful exercise of other rights secured by the Constitution and laws of the United States."

But as the *AP* points out in its report, a DOJ spokeswoman "said the policy applied only to unmanned aircraft systems rather than piloted airplanes."

"These are not your grandparents' surveillance aircraft," Jay Stanley, a senior policy analyst with the American Civil Liberties Union, told the *AP*.

The flights are significant "if the federal government is maintaining a fleet of aircraft whose purpose is to circle over American cities, especially with the technology we know

can be attached to those aircraft," Stanley said.

FBI Spied 'Beyond Its Authority' on Keystone XL Opponents

Published on Tuesday, May 12, 2015 by Common Dreams by Nadia Prupis, staff writer

The Federal Bureau of Investigation (FBI) broke its own internal rules when it spied on Keystone XL opponents in Texas, violating guidelines designed to prevent the agency from becoming overly involved in complex political issues, a new report by the *Guardian* and*Earth Island Journal* published Tuesday has revealed.

Internal documents acquired by the outlets through a Freedom of Information Act (FOIA) request show how the FBI failed to get approval for launching investigations into Houston-based protesters, whom the agency labeled "environmental extremists," and held a bias in favor of the controversial tar sands pipeline—currently awaiting federal approval—extolling its supposed economic benefits in one document which outlined reasons for spying on its opponents.

"Many of these extremists believe the debates over pollution, protection of wildlife, safety, and property rights have been overshadowed by the promise of jobs and cheaper oil prices," the file states. "The Keystone pipeline, as part of the oil and natural gas industry, is vital to the security and economy of the United States."

The *Guardian* reports:

> *Between November 2012 and June 2014, the documents show, the FBI collated inside knowledge about forthcoming protests, documented the identities of individuals photographing oil-related infrastructure, scrutinised police intelligence and cultivated at least one informant.*
>
> *….However, the partially redacted documents reveal the investigation into anti-Keystone activists occurred without prior approval of the top lawyer and senior agent in the Houston field office, a stipulation laid down in rules provided by the attorney general.*

Additionally, the FBI appeared to have opened its file on the Keystone XL opponents in 2013 following a meeting between officials from the agency and TransCanada, the company building the pipeline.

"For a period of time—possibly as long as eight months—agents acting beyond their authority were monitoring activists aligned with [direct action climate group] Tar Sands Blockade," the *Guardian* writes.

Dozens of activists were arrested in Texas in late 2012, although none were accused of violent crime or property damage, according to key Tar Sands Blockade organizer, Ron Seifert.

"Less than a month after TransCanada showed the FBI a PowerPoint claiming that people opposed to [Keystone XL] need to be watched, Houston's FBI office cuts corners to start an investigation; it's not surprising but it is revealing of who they really work for," Seifert told*Common Dreams* on Monday. "The FBI has been harassing and actively repressing communities of organizers for decades."

Yet more records show that the FBI associated the Tar Sands

Blockade, which organizes peaceful protests, with other "domestic terrorism issues."

Other documents suggest that the Houston-based investigation was only one of a larger probe, possibly monitoring other anti-Keystone XL activists around the country.

"We're not surprised," Seifert continued. "We're also not deterred. Movements for climate and environmental justice are activating people from diverse political backgrounds to take direct action to defend themselves from threats like [Keystone XL]. People are stepping out of the blind alleys of electoral politics and building grassroots power, and that's scary for people who want a monopoly on power."

After NSA Ruling, Congress at Odds Over Mass Surveillance

Published on Friday, May 08, 2015 by Common Dreams by Nadia Prupis, staff writer

In the wake of Thursday's federal court ruling that the U.S. National Security Agency's mass data collection program is illegal, officials in Congress have been left at odds over surveillance reform.

In the remaining six days of the legislative session, some Senate Republicans are rushing to find a short-term solution to keep the program in operation until it comes to the floor for a vote—one which is unlikely to pass in light of the court ruling. The government previously held that Section 215 of the Patriot Act, set to expire on June 1, justified the NSA's mass

surveillance of U.S. citizens.

One option would be a one-month extension of the provision to get it past the deadline in exchange for Republicans allowing a vote on the USA Freedom Act—a bill aimed at reforming the NSA by replacing surveillance programs with a plan for phone companies to retain data instead. Some in Congress see the USA Freedom Act as their best chance to rein in the NSA's spying powers.

"I hope we can [pass a clean reauthorization] for at least a short period of time just so we can have this debate," majority whip Sen. John Cornyn of Texas told reporters. "It's an important debate and an important law, it's protected Americans and saved lives, and so we don't need to make this decision in haste."

That statement conflicted with Sen. Mitch McConnell's (R-KY) response to Thursday's court ruling, which he said should not impede a full reauthorization of the act. The provisions are "ideally suited for the terrorist threat we face in 2015," McConnell said.

However, the call to reject the Patriot Act has grown stronger, with allies from both sides of the aisle framing the court ruling as a turning point in the debate.

Even a short-term extension would amount to "reauthorizing for five years a statute that right now is deeply flawed," Sen. Richard Blumenthal (D-Conn.) told the *Guardian*. "It fails to protect essential rights and clearly could be improved by having an adversarial system for example, changing the makeup of the [Fisa] court, reforming the system as needs to be done."

Sen. Rand Paul (R-KY), a presidential candidate for the 2016 election, wrote in an op-ed for*Time* that not even the USA Freedom Act is enough to reform the NSA and should be rejected alongside the Patriot Act. "Now that the appellate court has

ruled that Section 215 doesn't authorize bulk collection, would the USA Freedom Act actually be expanding the Patriot Act?" he wrote. "That would be a bitter irony if the attempt to end bulk collection actually gave new authority to the Patriot Act to collect records."

The American Civil Liberties Union (ACLU), which brought the case to the federal court, has also noted that the USA Freedom Act does not go far enough to rein in the government's surveillance powers or ensure sufficient transparency from the FBI. "We can't help but worry that the vague language in the bill's key provisions will provide a new lease on life to surveillance programs that haven't yet been—and may never be—disclosed to the public," wrote ACLU deputy legal director Jameel Jaffer and ACLU staff attorney Patrick Toomey in a blog post last week, ahead of the ruling.

On Thursday, the ACLU called the court's decision a "resounding victory for the rule of law."

Staff attorney Alex Abdo, who argued the case, said in a statement, "For years, the government secretly spied on millions of innocent Americans based on a shockingly broad interpretation of its authority…. Mass surveillance does not make us any safer, and it is fundamentally incompatible with the privacy necessary in a free society."

Big and Small, Near and Far…

The Drones Are Coming

Published on Tuesday, May 05, 2015 by Common Dreams by Jon Queally, staff writer

Near and far… the proliferation of drones is coming.

With the Federal Aviation Administration facing pressure from corporate interests and drone manufacturers to make room in the skies over the United States, the push for industry-friendly regulations is now in full gear.

Meanwhile, foreign governments are rapidly developing their own technology to make sure the era of the unmanned aircraft—so far dominated by the U.S. military—does not leave them stranded on the ground, both literally and strategically.

Though critics of the U.S. government's use of drones on foreign battlefields (not to mention over foreign nations with whom the U.S. is not at war) have focused on human rights violations and international law, the concern over domestic drones has been more intent on addressing privacy issues and the threat that so-called "full spectrum surveillance" could ultimately have on society. But with the FAA now considering new rules that would regulate the use of recreational and commercial drones, the corporate lobbyists are in full swing to make sure those rules conform to their vision of new profit streams.

As *Bloomberg* reports, some of the nation's largest companies—including Amazon, American International Group Inc., Chevron Corp. and BNSF Railway Co.—have no intention of letting the opportunity pass them by:

> *While Amazon works on futuristic cargo carriers, other companies are seeking less-restrictive rules as they begin to get unmanned aerial vehicles into U.S. skies.*
>
> *"I don't think any of us are out to do this because it's a*

> *cool thing to do," Lynden Tennison, Union Pacific's chief information officer, said in an interview. "We're out to do it because we believe it has business benefits."*
>
> *Drones' potential will be a centerpiece this week in Atlanta as manufacturers and users gather for the annual trade show for the Association for Unmanned Vehicle Systems International. The FAA will be urged to move quickly on permanent rules.*

At the same time, *Business Insider*, journalist Jeremy Bender describes how other industrial powers—namely China, Russia and other military powerhouses—are hard at work developing their own technology to compete with the U.S.:

> *The US, which has been at the forefront of unmanned aerial vehicle technology, will soon have to adjust to a world in which a wide range of armed forces and potential adversaries have drones as well.*
>
> *According to Ian Bremmer, president of political-risk consultancy Eurasia Group, the technological gap that allowed the US to enjoy coercive diplomatic advantages over its rivals is rapidly shrinking. Drones are no exception.*
>
> *"China has moved the most quickly to develop significant drone capabilities and will start deploying them to support their national security capabilities," Bremmer wrote in a recent note provided to Business Insider.*
>
> *"China will also face much the same backlash from the international community as we start to see unintended civilian casualties as a consequence of expansive Beijing-led drone use," he added. "But it will set off the strong proliferation of another disruptive technology."*

Snowden Docs Reveal Canada a Major Player in Global Spy Operations

Published on Monday, March 23, 2015 by Common Dreams
by Lauren McCauley, staff writer

Canada's spy agency, the Communication Security Establishment (CSE), is a major player in global hacking operations and boasts a vast array of cyberwarfare tools, revealed in news reports on Monday, that rivals that of the United States' National Security Agency.

Documents initially leaked to the *Intercept* by Edward Snowden and now reported on in collaboration with the *CBC* show that the NSA and its northern counterpart "cooperate closely" in "computer network access and exploitation" of certain international targets. According to one document, an April 2013 briefing note for the NSA, targets are located in the Middle East, North Africa, Europe and Mexico, in addition to unnamed countries allegedly connected to the two agencies' counterterrorism goals.

Another document, a 2011 presentation by a CSE analyst, outlines the vast array of Canadian cyber-spy capabilities. According to the *CBC*, many of these tactics go beyond hacking for intelligence, including: "destroying infrastructure, which could include electricity, transportation or banking systems; creating unrest by using false-flag –ie. making a target think another country conducted the operation; disrupting online traffic by such techniques as deleting emails, freezing internet connections, blocking websites and redirecting wire money transfers."

Ronald Deibert, director of the Citizen Lab at University of Toronto's Munk School of Global Affairs, told *CBC* that these revelations should serve as a "major wakeup call for all Canadians," especially as the country's parliament weighs a sweeping and controversialnew counter-terrorism bill, C-51.

"These are awesome powers that should only be granted to the government with enormous trepidation and only with a correspondingly massive investment in equally powerful systems of oversight, review and public accountability," says Deibert.

Wikimedia vs. NSA: Major Lawsuit Challenges Government Surveillance of US Citizens

Published on Tuesday, March 10, 2015 by Common Dreams
by Jon Queally, staff writer

Wikipedia, the online encyclopedia and one of the most highly-trafficked websites in the world, announced Tuesday that it—alongside a host of civil liberty advocates, news outlets, and privacy rights organizations—has filed a lawsuit against the National Security Agency for violating the constitutional rights of its users by performing bulk surveillance and searching, without specific cause or warrant, the international Internet communications of all Americans including emails, web-browsing content, and search-engine queries.

The lawsuit, named as *Wikimedia v. NSA,* was filed by the ACLU on Tuesday. In addition to the Wikimedia Foundation (of which

Wikipedia is a part), the other plaintiffs include: the conservative Rutherford Institute, The Nation magazine, Amnesty International USA, PEN American Center, Human Rights Watch, the National Association of Criminal Defense Lawyers, Global Fund for Women, and Washington Office on Latin America.

Filed in federal court in Maryland where the NSA is headquartered, the lawsuit (pdf) argues that the NSA is violating the plaintiffs' privacy rights under the Fourth Amendment and infringing on their First Amendment rights. The complaint also argues that what is called "upstream surveillance"—mass surveillance on all communications that pass through certain "backbone" structures of the network—exceeds the authority granted by Congress under the FISA Amendments Act.

The complaint reads, in part:

> *This lawsuit challenges the suspicionless seizure and searching of internet traffic by the National Security Agency ("NSA") on U.S. soil. The NSA conducts this surveillance, called "Upstream" surveillance, by tapping directly into the internet backbone inside the United States – the network of high-capacity cables, switches, and routers that today carry vast numbers of Americans' communications with each other and with the rest of the world. In the course of this surveillance, the NSA is seizing Americans' communications en masse while they are in transit , and it is searching the contents of substantially all international text-based communications – and many domestic communications as well – for tens of thousands of search terms.*

"By tapping the backbone of the Internet, the NSA is straining the backbone of democracy," said Lila Tretikov, executive director of the Wikimedia Foundation. "Wikipedia is founded on the freedoms of expression, inquiry, and information. By violating our users' privacy, the NSA is threatening the

intellectual freedom that is a central to people's ability to create and understand knowledge."

Largely exposed to the general public through internal NSA documents leaked by whistleblower Edward Snowden and a steady stream of investigative reporting based on his disclosures, the groups object to how the NSA copies and combs through vast amounts of Internet traffic, which it intercepts inside the United States with the help of major telecommunications companies. According to the ACLU, the surveillance involves the NSA's warrantless review of the emails and Internet activities of millions of ordinary Americans.

"This kind of dragnet surveillance constitutes a massive invasion of privacy, and it undermines the freedoms of expression and inquiry as well," said ACLU staff attorney Patrick Toomey. "Ordinary Americans shouldn't have to worry that the government is looking over their shoulders when they use the Internet."

In an op-ed in the *New York Times* published Tuesday to coincide with the announcement of the lawsuit, Tretikov and Jimmy Wales, the founder of Wikipedia, explain the reasoning behind the legal challenge. "Our lawsuit," they write, "says that the N.S.A.'s mass surveillance of Internet traffic on American soil—often called 'upstream' surveillance—violates the Fourth Amendment, which protects the right to privacy, as well as the First Amendment, which protects the freedoms of expression and association. We also argue that this agency activity exceeds the authority granted by the Foreign Intelligence Surveillance Act that Congress amended in 2008."

Because Wikipedia and other online services provided by the larger Foundation are viewable to the public "anonymously"—that is, without the need to create a user account or log in—and because many of the volunteers who maintain entries on the site do so with a distinct desire *not* to be monitored, Wales and Tretikov argue those people should

“be able to do their work without having to worry that the United States government is monitoring” the content they’re accessing or their related online behavior.

“Unfortunately,” write Wales and Tretikov, the anonymity of Wikipedia users “is far from certain because, using upstream surveillance, the N.S.A. intercepts and searches virtually all of the international text-based traffic that flows across the Internet ‘backbone’ inside the United States.”

According to the ACLU:

> *The lawsuit is in some ways a successor to a previous ACLU lawsuit challenging the NSA’s warrantless wiretapping program, Clapper v. Amnesty. The Supreme Court dismissed that case in February 2013 in a 5-4 vote on the grounds that the plaintiffs could not prove that they had been spied on. Edward Snowden has said that the ruling contributed to his decision to expose certain aspects of the NSA’s surveillance activities a few months later.*
>
> *Among the Snowden disclosures were documents relating to upstream surveillance, which has since been confirmed by the government. Unlike the surveillance considered by the Supreme Court in Clapper, upstream surveillance is not limited to the communications of NSA targets. Instead, as we have since learned, the NSA is searching the content of nearly all text-based Internet traffic entering or leaving the country — as well as many domestic communications — looking for thousands of keywords such as email addresses or phone numbers.*
>
> *One of the NSA documents revealed by Snowden included a slide that named Wikipedia, among other major websites, as a good surveillance target for monitoring what people do on the Internet.*

As Toomey wrote in a blog post about the lawsuit on Tuesday, “Upstream surveillance flips the Constitution on its head. It

allows the government to search everything first and ask questions later, making us all less free in the process. Our suit aims to stop this kind of surveillance."

Snowden Document Reveals Huge Scope of Canada's Domestic Surveillance

Published on Wednesday, February 25, 2015 by Common Dreams
by Lauren McCauley, staff writer

Canada's electronic spy agency, the Communications Security Establishment (CSE), collects millions of emails and other information from its citizens and stores them for "days to months," according to a document leaked by NSA whistleblower Edward Snowden and revealed by *CBC News* in collaboration with *The Intercept* on Wednesday.

According to the top-secret CSE document, analysts "watched visits to government websites and collected about 400,000 emails to the government every day, storing some of the data for years," *CBC* reports.

Such online activity includes Canadians filing taxes, writing to members of Parliament and applying for passports. The sweeping data collection is being carried out in an alleged effort to protect government computers.

Using a tool called PonyExpress, the surveillance agency scans the documents for "suspicious links or attachments." The 2010 document reveals that the system detects about 400 potentially

suspect emails each day, or roughly 146,000 each year, though only about four emails a day warrant CSE analysts contacting government departments directly.

The document indicates that the scale of the data collection has likely increased since that time. Under a heading marked "future," the document notes: "metadata continues to increase linearly with new access points."

"It's pretty clear that's there's a very wide catchment of information coming into [CSE]," Micheal Vonn, policy director at the British Columbia Civil Liberties Association, told the *CBC.*

The document reveals that CSE is storing large amounts of "passively tapped network traffic" for "days to months," including email content, attachments and other online activity, *The Intercept* reports, while some forms of metadata is kept for "months to years."

"When we collect huge volumes, it's not just used to track bad guys," Chris Parsons, an internet security expert with internet think tank Citizen Lab, who viewed the document, told the *CBC.* "It goes into data stores for years or months at a time and then it can be used at any point in the future."

A previously leaked document revealed in 2013 that CSE intercepts citizens' private messages without judicial warrants. After that, CSE acknowledged it collected some private communications but did not divulge the amount being stored or say for how long. Now, *The Intercept* reports, "the Snowden documents shine a light for the first time on the huge scope of the operation—exposing the controversial details the government withheld from the public."

The Intercept report continues: "Under Canada's criminal code, CSE is not allowed to eavesdrop on Canadians' communications. But the agency can be granted special ministerial exemptions if its efforts are linked to protecting government

infrastructure—a loophole that the Snowden documents show is being used to monitor the emails."

Google Draws Wikileaks' Ire for Secretly Providing Private Email Data to DOJ

Published on Monday, January 26, 2015 by Common Dreams
by Jon Queally, staff writer

In what non-profit media organization Wikileaks is calling a "horrifying precedent for press freedoms," internet giant Google has confirmed it complied with a request by the U.S. government to hand over the complete content and data attached to email accounts belonging to three Wikileaks staffers under a secret search warrant issued by a federal judge in 2012.

On Sunday, attorneys representing Wikileaks sent a letter (web) to executives at Google demanding answers related to what they termed the "serious violation of the privacy and journalistic rights" of their three employees—Investigations editor Sarah Harrison, Section Editor Joseph Farrell and senior journalist and spokesperson Kristinn Hrafnsson.

"The broadly tailored search warrants are evidence of the fact that the government refuses to recognize that WikiLeaks is staffed by journalists and editors. It refuses to recognize that the organization's act of publishing US government documents is an act of journalism." —Kevin Gosztola, FireDogLake

Wikileaks was notified on Christmas Eve of 2014 by Google that the order had been fulfilled, citing a gag order the company said prevented it from informing the three individuals, or their employer, earlier. Wikileaks is only making the details of the situation public now.

The letter from Wikileak's legal team to Google's chairman Eric Schmidt states, "We are astonished and disturbed that Google waited over two and a half years to notify its subscribers that a search warrant was issued for their records."

According to Wikileaks, the warrants reveal for the first time a clear list of the alleged offenses the US government is trying to apply in its attempts to build a prosecution against Julian Assange and his staff for their role in revealing secrets that have proved damaging to the nation's reputation. The possible criminal offenses cited by the order, according to the group's analysis, could total 45 years of imprisonment.

Assange, in a statement, aimed his ire at the White House for seeking out access to the private communications. "WikiLeaks has out endured everything the Obama administration has thrown at us," Assange said, "and we will out endure these latest 'offenses' too."

Though Wikileaks has said that its staffers do not use their gmail accounts for communications related to their work, the group argues the search warrants represent a clear violation of their personal privacy and an assault on press freedoms.

For her part, Sarah Harrison told the *Guardian*, "Knowing that the FBI read the words I wrote to console my mother over a death in the family makes me feel sick."

The Guardian reports:

> *When it notified the WikiLeaks employees last month, Google said it had been unable to say anything about the warrants*

earlier as a gag order had been imposed. Google said the non-disclosure orders had subsequently been lifted, though it did not specify when.

Harrison, who also heads the Courage Foundation, told the Guardian she was distressed by the thought of government officials gaining access to her private emails. […]

She accused Google of helping the US government conceal "the invasion of privacy into a British journalist's personal email address. Neither Google nor the US government are living up to their own laws or rhetoric in privacy or press protections".

The court orders cast a data net so wide as to ensnare virtually all digital communications originating from or sent to the three. Google was told to hand over the contents of all their emails, including those sent and received, all draft correspondence and deleted emails. The source and destination addresses of each email, its date and time, and size and length were also included in the dragnet.

According to the statement from Wikileaks:

WikiLeaks' legal team has written to Google expressing its dismay that Google failed to notify the warrants' targets immediately. The failure to notify has prevented the three journalists from "protect[ing] their interests including their rights to privacy, association and freedom from illegal searches". The "take everything" warrants are unconstitutionally broad and appear to violate the Privacy Protection Act so would have a good chance of being opposed; however, Google handed everything over before that was possible.

Although Google claims that it was at some stage under a gag order from the US government, there is no indication that Google fought the gag and it is unlikely that the gag just

> *happened to expire the day before Christmas. Similar gags for warrants against WikiLeaks journalists have been successfully fought by Twitter in much shorter time-frames.*
>
> *While WikiLeaks journalists, perhaps uniquely, do not use Google services for internal communications or for communicating with sources, the search warrants nonetheless represent a substantial invasion of their personal privacy and freedom. The information handed over to the US government included all email content, metadata, contacts, draft emails, deleted emails and IP addresses connected to the accounts. Google redacted the search warrants before sending them to WikiLeaks staff.*

Speaking with the *Guardian*, Alexander Abdo, a staff attorney and privacy expert at the American Civil Liberties Union, said the warrants were "shockingly broad" and deeply troubling.

"This is basically 'Hand over anything you've got on this person'," Abdo told the Guardian. "That's troubling as it's hard to distinguish what WikiLeaks did in its disclosures from what major newspapers do every single day in speaking to government officials and publishing still-secret information."

Journalist Kevin Gosztola, writing at *FireDogLake*, expanded on this point. "The broadly tailored search warrants are evidence of the fact that the government refuses to recognize that WikiLeaks is staffed by journalists and editors. It refuses to recognize that the organization's act of publishing US government documents is an act of journalism."

The implications of this, according to Gosztola, are profound. He explained:

> *Imagine the US government had served search warrants on the editors of The New York Times. Imagine Google received these warrants, and they were as broad as the ones issued against WikiLeaks editors—and Google did not fight back. The entire*

> *US press corps would be livid, as they rightfully were when it became known that the Justice Department had seized the Associated Press' phone records for a leak investigation.*
>
> *In fact, the government recently concluded their relentless pursuit of Times reporter James Risen. They spent years arguing in court that he had no reporter's privilege and had to reveal his confidential sources so the government could prosecute former CIA officer Jeffrey Sterling for a leak. They seized many of records of his personal communications and even some detailing financial transactions.*
>
> *While comparatively there may be more of a political cost to the Justice Department if they were to go after The New York Times, one never knows when there might be a presidential administration that does not buckle to public pressure, as was the case with Risen. The legal precedents created as the government pursues WikiLeaks are the same legal precedents that can always be used to go after other journalists in the future. American journalists maintain their collective silence at their profession's own peril.*

In his statement released on Sunday, Assange said, "I call on president Obama to do the right thing and call off his dogs—for his own sake. President Obama is set to go down in history as the president who brought more bogus "espionage" cases against the press than all previous presidents combined."