GlobalResearch
Center for Research on Globalization

High Tech Surveillance: U.S. Internal Revenue Snooping Social Media and Emails Without Warrant

By Clarence Walker
Global Research, April 24, 2013

Region: USA
Theme: Intelligence, Police State & Civil Rights

Americans have a big problem with the IRS (Internal Revenue Service). If anyone discuss the filing of tax return in their emails the IRS may be monitoring what you say to see if you may be trying to cheat on taxes, committing money laundering or sending non-reported funds to tax havens.

Americans are under siege by questionable U.S. government surveillance tactics, tactics that pry into people's daily life even when no crime may have occurred. In the past FBI and DEA (Drug Enforcement Administration) have used warrantless GPS tracking devices to track vehicles and the latest "Stingray" tracker have been used to listen in on cell phone communication to

pinpoint a person's location, including the extraction of cell data like text messages, which numbers were called–all done without a warrant in violation of the Fourth Amendment Constitution prohibiting "Unreasonable Search and Seizure."

In U.S. v Antoine Jones the Supreme Court in Washington ruled in January 2012 that federal government illegally tracked Jones, a suspected drug trafficker, for 28 days, without a warrant. This Fourth Amendment violation resulted in Jones life without parole conviction reversed for retrial. In a new trial held this year, Jones represented himself and won a 6-6 hung jury. No date been set for another trial.

Now the IRS is the latest to jump on the government bandwagon of spying on the emails of American citizens who file tax returns, without a warrant! According to a lawsuit filed by ACLU(American Constitution League Union)–the IRS released documents explaining why their agents didn't need a warrant to read other people's emails to detect whether or not if someone liable to violate U.S. tax laws by under reporting their earnings. Suspected drug drug dealers and money launderers who use the internet to transact illegal business online are prime targets as well.

Example of IRS monitoring drug organizations who use the internet and other forms of wireless communication to launder proceeds, IRS Special Agent Andre Guilot said the Quality Express Convenience Store in Baton Rouge Louisiana owned by Thang Minh "Tommy" Tran laundered over $170 million dollars of drug money into Hancock Bank between July 2006

and December 2011. Other members of the conspiracy were identified as Son "Tatto" Nguyen of Baton Rouge and Thahn "Money" Nguyen of New Orleans. Wire transfers and emails showed the men transferred $275,000 in narcotic proceeds into a Houston Texas

location.

IRS deny reading emails without a warrant by issuing a recent public statement:

> "The IRS does not use emails to target taxpayers; any suggestions to the contrary is wrong."

Documents obtained by ACLU prove otherwise. In one leaked memo, IRS lawyers told their agents that

> "Non consensual monitoring or electronic communications….can be used to investigate a federal felony." "Further, the Chief Counsel, said, "Emails and other transmissions lose their reasonable expectation of privacy and Fourth Amendment protection once emails been sent from an individual's computer."

The Wall Street Journal reports "the IRS can also monitor Facebook and Twitter accounts outside of an investigation like targeting people suspected of lying on their tax returns- or targeting private emails of suspected narcotic dealers which as a rule the IRS realize most criminals don't usually pay taxes on illicit funds, but in essence, most suspected lawbreakers use cell phones, emails and emails to carry out crimes. IRS direct order to their agents to snoop on citizens emails are in the crossfire of judges, legislators, privacy groups and attorneys across the nation.

IRS is able to execute this scheme due to the outdated ECPA law(Electronic Communication Privacy Act) which allows government agencies to obtain emails more than 180 days old although the leeway to do so can easily run afoul of the Fourth Amendment protection because whose to say the government will follow strict legal guidelines.

As the firestorm brew over email and social media privacy, and even if the IRS accessed warrantless emails the tactic may soon end in glorious defeat. U.S. Senate are currently working overtime on rewriting the law to update the ECPA that will require government agencies to have a warrant to open and read emails in any form.

Critics insists that Americans' email messages should be protected from warrantless search and seizures. The prevailing theory is this: emails and social media messages should have the same Fourth Amendment privacy standards as that of a "hard drive" located on someone's computer inside a locked residence including paperwork stashed in a vault or filing cabinet.

"What the IRS is doing to emails is a massive invasion of privacy", says Houston Texas-based Tax lawyer expert Michael Minns. Minns is the author of the best-selling book: "The Underground Lawyer." Minns is a lifelong advocate of the Fourth Amendment, a fearless legal crusader, who represent people charged with IRS tax crimes. "Since IRS have been monitoring emails without a warrant this is very troubling and it violates the Fourth Amendment." Minns recall previous court trials of people charged with IRS crimes, and the lawyers and their clients often wondered how IRS knew about certian conversations regarding sensitive information discussed privately online.

"So how long this really been going on?" Minns questioned.

Meanwhile U.S. Congress members are demanding answers from the IRS. In a letter sent to

the IRS on April 11th, Republican Louisiana Representative Charles Boustany, the Chairman of the House Committe on Ways and Means on Oversight; Boustany demanded answers from IRS about its policy on searching emails and other electronic communications; how many emails have been searched without a warrant within the last several years; and specifically what the agency was looking for. “They made some statement about targeted searches, but they have not specifically addressed what was asked in our letter,” Congress Press Secretary Sarah Swinehart told the Washington Whisper.

IRS spokesman Dean Patterson told the Whisper that he believes the agency “will say more on the issue”. Patterson declined to say what or when.

Writing in the U.S. News and Reports, Rick Newman defends the IRS. Newman says the American people should appreciate the benefits of a stable tax system and tough enforcement of tax rules. “The U.S. Treasury borrow money at interest rates of less than 2 percent for a 10 year loan that benefit Americans in many ways: “It keeps government spending higher than it would–which funnels money to many businesses and help the economy grow. Low rates on government securities, Newman points out, also keeps rates low on consumer loans making homes, cars and other things more affordable.”

“What happens to nations with lax tax systems. Greece, for one, suffers from an epidemic of tax cheating that helped send the nation to the brink of bankruptcy while causing a full blown depression,” Newman wrote in the News Report article published on April 12th 2013.

Privacy Rights Upheld in U.S. VS Steven Warshak

One case involving the IRS obtaining warrantless emails involves the case of Steven Warshak. On December 14th 2010, Federal Court Sixth Circuit held that “government agents violated Warshak’s Fourth Amendment rights by compelling his ISP(Internet Service Provider) to hand over Warshak’s emails without first obtaining a search warrant based on probable cause.” A Federal Judge allowed prosecutors to introduce the emails as evidence during trial because the IRS agents testified they acted in good faith under the ECPA Stored Communications Act.

Sixth Circuit further ruled: “Given the fundamental similarities between email and traditional forms of communication, it would defy common sense to afford emails lesser Fourth Amendment protection.”

Seeking taxes on approximately $250 million dollars that Warshak made with his business called Berkeley Premium Nutraceuticals the IRS seized Over 27,000 emails belonging to the prominent businessman. Warshak decision is important because the Sixth Circuit is the first court from the U.S. Court of Appeals to explicitly rule there is a “reasonable of expectation of

privacy in the content of emails stored on a third-party server and that the emails wee subject to Fourth Amendment protection. Privacy activists hailed this decision as a standard bearer for the Fourth Amendment protection of electronic communications. Yet the IRS ignored the decision by upping the ante relying on an updated edition of its Search Warrant Handbook that ordered their agents to continue on as they were in “obtaining everything in an account except for unopened email or voice mail stored with a provider for 180 days or less without a warrant.”

This defiant order was supported by a memo sent out in October 2011 by IRS Senior Counsel William Spatz. Spatz argued in the document that the IRS should comply by the ruling of the Ninth Circuit and that "The Ninth Circuit and other courts have recognized that a warrant is not required for government entity to require an electronic provider to produce a customer's electronic communication."

High Tech Tracking Tools: How Much IRS Really Know About American Citizens

Under fire by DOJ(Department of Justice) to help dig the government out of a budget crisis the IRS has geared up to track down approximately over $300 billion dollars in revenue lost to evasions, illegal money laundering and tax cheats. Faced with evolving technology used by millions of computer users the IRS recently announced the agency will start using "robo audits" of tax forms and third-party data to bridge a "tax gap." Former IRS Commissioner Douglas Shulman said in a public statement "that the technology will employ billions of pieces of data to target enforcement of noncompliance."

"It's not clear what they are using and how," says Bill Smith, a manager director at the accounting firm CBIZ MHM. "But don't brag on Facebook about how you are cheating. The IRS can see that." "It's well known in the tax community, but not many people outside of it, are aware of this big expansion of data and computer use," says Edward Zelinsky, a tax law expert and professor at Benjamin Cardozo School of Law. "I am sure people will be concerned about the use of personal information ion databases in government." "Taypayers should know, Zelinsky adds, that whatever people do and say electronically can and will be used against them in IRS enforcement."

Most Americans are familiar with "internet cookies" that silently track human interaction online which provides direct leeway for targeted "ads" to pop up when a user switch from one website to another. But IRS has hired private industry experts to employ similar digital tracking with a major advantage to easily access social security numbers, health records, credit card transactions, ebay and Amazon purchases including other private information that marketers and different elite businesses don't generally see.

"Private industry would be envious if they knew what our models are," boasted Dean Silverman, as reported in trade publications. Silverman is the high-tech specialists who heads a group of recruited private sectors to update IRS technology to snoop on citizens using the internet. As expected the IRS declined to comment to national mainstream journalists on how they will use the new technology to sniff out online tax cheats. According to U.S. News and Report–IRS officials has already outline their plan in partnership with IBM and EMC to use their new technology for the following:

(1) Charting and analyzing emails and Social Media like Facebook, Twitter and Linkedin.

(2) Targeting audits by matching tax filings to Social Media or electronic payments.

(3) Tracking individual internet addresses and emailing patterns.

(4) Sorting data in 32,000 categories of metadata and 1 million unique "attributes."

(5) Maching learning across "neutral" networks.

Can Americans Avoid IRS Internet Trap?

Tax law experts provides the following tips to aid citizens to avoid the IRS "big trap" on the internet. These tips may not be foolproof but they are considerable safeguards:

(1) Double check your online postings and emails against your tax filings to insure the information is accurate.

(2) Don't brag to friends online about extra financial benefits that you received, then forget to list it on your tax returns. IRS can detect this.

(3) Be aware that professional tax preparers store information online is subject to IRS surveillance. So make sure the numbers are correct.

Another danger signal is when people use anonymous online "cloud drop boxes" or anonymous email addresses. Experts say these techniques are not safe-proof, particularly for drug dealers who launder money to tax havens and other shady laundering operations. Former CIA Director David Petraeus can attest to this unequivocal fact when he attempted to conceal a steamy romance. FBI zeroed in on Petraeus's dropbox that stil contained his emails with his mistress. and the affair were exposed when investigators accessed the emails from Petraeus's online storage space–although he mistakenly thought the information had been deleted.

"Anonymous postings depends on what sort of investigation is done," said Bruce Schneir, Chief Security Technology Officer at BT, a British telecommunications company. "The FBI and by extension of the IRS, could obtain the data on a specific person."

Overall, most important, perhaps we should not vilify the IRS for the convoluted, often confusing tax code. Congress creates the tax laws and the IRS enforces them. But the tax code

doesn't allow intentional violation of the Fourth Amendment against unreasonable search and seizures. The IRS should promptly reply to lawmakers questions abut their warrantless snooping of emails and social media conversations. Even more important the IRS should formally modify their policies to require agents to obtain warrants to access emails irrespective of how old or how new the emails may be.

Final analysis: It will take Congress to rewrite the ECPA laws to prevent IRS exploitation of the Stored Communication Act to swipe emails at their disposal. The American Constitution should never be compromised or taken for granted, but when the government wants to deprive its citizens of liberty and freedom it's like they are saying: "Federal government giveth and the federal government taketh it away."

Articles by: **Clarence Walker**