ELECTRONIC FRONTIER FOUNDATION

From EFF's Secret Files: Anatomy of a Bogus Subpoena

November 2009

How the Government Secretly Demanded the IP Address of Every Visitor to Political News Site Indymedia.us

1. Introduction: Lifting the Fog of Secrecy Surrounding Law Enforcement Surveillance

Table Of Contents

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. (For more background on how the SCA works, see this section of EFF's Surveillance Self-Defense manual.)

We at EFF, like the public at large, are often left in the dark about what the government's practices in this area look like. However, sometimes — just sometimes — the fog will clear and we'll get a worrisome picture of what the government gets up to behind closed doors. Sometimes this happens when an independent-minded judge publishes an opinion revealing the government's practices, like the judge that first revealed that the government was tracking cell phones without warrants. Other times, someone served with an SCA demand such as a National Security Letter comes to us for legal assistance.

Recently, one such recipient of an SCA demand did come to us, and we're glad she did. The story of that subpoena — to the administrator of www.indymedia.us, an independent activist news site aggregating stories from Indymedia web sites across the country — provides yet another example of how government abuses breed in secrecy. Hopefully this analysis will be helpful to other online service providers who receive such bogus requests masquerading as valid legal process.

2. The Subpoena to Indymedia

On January 30th, 2009, Kristina Clair of Philadelphia, PA — one of the system administrators of the server that hosts the indymedia.us site — received in the mail a grand jury subpoena from the Southern District of Indiana federal court. The FBI had sent an email to Ms. Clair a couple of weeks earlier asking where a subpoena directed at the indymedia.us site should be sent. So, we at EFF were ready and waiting to evaluate the subpoena as soon as it arrived. Yet even we were surprised at what we saw. A PDF of the entire subpoena is available here.




3. The Indymedia Subpoena's Flaws: Demanding "all IP traffic to and from www.indymedia.us"

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. This sample subpoena from the Justice Department's surveillance manual shows what the government typically asks for, tracking the statute's language.

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."

Please provide the following information pursuant to Title 18, United States Code, Section 2703(c)(2):

All IP traffic to and from www.indymedia.us (65.23.159.255), June 25, 2008. Include IP addresses, times, and any other identifying information

1. All customer or subscriber account information for any accounts registered to the following username or identification number:

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 of *every* Indymedia reader of *every* Indymedia story was relevant to the crime being investigated by the grand jury in Indiana, whatever that crime may be.

4. The Indymedia Subpoena's Flaws: The Bogus Gag Order Demanding the Recipient's Silence Without Any Legal Basis

The government added insult to injury by also inserting this language on the first page of the subpoena: "You are not to disclose the existence of this request unless authorized by the Assistant U.S. Attorney. Any such disclosure would impede the investigation being conducted and thereby interfere with the enforcement of the law."

You are not to disclose the existence of this request unless authorized by the Assistant U.S. Attorney. Any such disclosure would impede the investigation being conducted and thereby interfere with the enforcement of the law.

The problem? The law *doesn't* require the recipient of a federal grand jury subpoena to keep the subpoena secret (which is why, typically, subpoenas often will "request" — but not require — a recipient's silence). There are certainly secrecy requirements for participants in the grand jury — such as the jurors and the prosecutors — but those requirements do not extend to witnesses (or potential witnesses such as a subpoena recipient). And although the SCA does provide the government with the option of obtaining a court order under 18 U.S.C. § 2705(b) requiring silence when the recipient's disclosure would have an adverse affect on an investigation, the government in this case did not obtain any such gag order.

In sum, without any legal authority to back up their purported gag demand, the government ordered Ms. Clair not to reveal the existence of the subpoena, a subpoena that as already described was patently overbroad and invalid under the SCA. This is exactly the kind of unjustified demand of silence that creates a fog around the government's often-overreaching surveillance activities. How many other subpoena recipients have remained silent over the years in response to such bogus demands, and how many of them violated their users' privacy by handing over data that the government wasn't entitled to? We simply do not know, and because of a lack of meaningful reporting about the government's use of the SCA, we cannot know.

We were determined that our client would not be one of the silenced, and that this illegal subpoena would eventually see the light of day.

5. EFF Responds to the Indymedia Subpoena; Government Backs Down

EFF decided to draft a letter to the Assistant US Attorney who issued the subpoena, laying out our concerns and refusing to comply with the subpoena's demands. This task was made all the easier by the fact that Indymedia.us, following EFF's suggestions in its "Best Practices for Online Service Providers", does not keep historic logs reflecting the IP addresses of its visitors. In other words, Indymedia didn't have what that the government was looking for.

Therefore, although we described all our various objections to the subpoena in EFF's first letter to the government, which was sent to Assistant US Attorney Doris L. Pryor on February 13, 2009, the main issue discussed in the letter was Indymedia's right to publicly discuss the subpoena.

In that letter, we explained that there was no legal basis for the subpoena's gag order, noted our intent to publish and critique the subpoena, and invited the government to seek a court order under the SCA's 18 U.S.C. § 2705(b) if it wished to maintain the subpoena's secrecy. We at EFF have long hoped to litigate whether such SCA gag orders violate the First Amendment, and this looked like it might be our opportunity.

However, the government declined our invitation. EFF's second letter to the government, addressed to a second Assistant US Attorney working on the case, Steven D. DeBrota, and cc'ing the first AUSA, Ms. Pryor, recounts what happened next:

> *On February 24, I received a voicemail from Ms. Pryor in response to my letter. In that message, Ms. Pryor said that I was correct that the subpoena did not compel Ms. Clair's silence, but that she would be seeking a*

court order, as she would confirm in a letter later that day.

This was a stunning admission: that the demand for silence in the subpoena had no legal basis, and that to legally compel silence the government would have to go to court for a gag order. The letter continues:

> *No such letter [confirming that the government would seek a gag order] was forthcoming; instead, I received on February 25 a faxed letter from Ms. Pryor simply stating that the subpoena had been withdrawn.*
>
> *Shortly after receiving that fax, on February 25, I and my colleague Lee Tien were able to reach you [i.e., the second AUSA, Mr. DeBrota] by phone to discuss the newly withdrawn subpoena.*
>
> *You indicated [during our phone conversation] that your office had reconsidered its position and, for unspecified reasons, was choosing not to seek a court order compelling Ms. Clair's silence. You further stated that your "legal posture" was that given the withdrawal of the subpoena, it was a "nullity" and that Ms. Clair "can say what she wants" — that there was "no legal disability" against Ms. Clair publicly discussing the subpoena. We expressed our pleasure at this and informed you of Ms. Clair's desire for EFF to publish the subpoena in conjunction with a legal critique of it, both to publicize an instance of government overreaching and to assist future recipients of similarly flawed subpoenas.*

Notably, before this phone call, the second AUSA — Mr. DeBrota — had left a flurry of voicemails with EFF on February 24th and 25th seeking to speak with us. Presumably, he wanted to clarify to us as soon as possible that the government would not be going to court to seek a gag order, so that we would not go to court ourselves based on AUSA Pryor's previous statement that it was going to go get a gag order. That previous statement likely would have given us a basis to go to court for an injunction to stop issuance of any gag order and, more importantly, bring an unprecedented challenge to the gag provision's constitutionality under the First Amendment. Obviously, that was a fight — and more importantly, a precedent — that the government wanted to avoid.

However, the phone conversation didn't end there. Instead, AUSA DeBrota still insisted that disclosure of the subpoena would harm the investigation, though he could not provide any specifics. These vague statements raised the spectre of our client being investigated or prosecuted for obstruction of justice for exercising her First Amendment right to publish and critique the subpoena. That is why, in an abundance of caution, we wrote the second letter. As that letter continues (emphases added):

> *Despite the choice not to seek a court order, you made clear your belief that disclosure of the subpoena would have an adverse impact on the grand jury's investigation, that it "may endanger someone's health" and would have a "human cost," and that Ms. Clair should use "conscience as her guide." When we pressed for you to confirm that Ms. Clair would face no legal consequences for her disclosure, e.g., prosecution by your office for obstruction of justice, you would not give it, instead noting the possibility of legal consequences if, for example, "her cousin is involved" in the conduct being investigated. To clarify the issue and memorialize our conversation, I emailed you and Ms. Pryor that same day confirming our understanding that there was no legal bar to Ms. Clair disclosing the subpoena. I received no response.*
>
> ***Your contradictory positions — your stated belief that disclosure of the subpoena will harm the investigation, contrasted with your failure to seek a court order based on that belief — are unacceptable.*** *Ms. Clair has not been informed of the nature of your investigation, the identity of its targets, or the nature of the crimes being investigated. Ms. Clair has no intent, corrupt or otherwise, to influence, obstruct, or impede the due administration of justice in this matter. She does, however, wish to exercise her First Amendment right to speak about the subpoena without restriction, and to authorize EFF to publish and critique the subpoena. Yet that speech has been chilled by the vague threat of obstruction of justice inherent in your imprecise and unsupported statements that her disclosure would somehow harm your investigation.*
>
> ***Put simply, you cannot have it both ways.*** *If you believe that Ms. Clair's disclosure of the*

subpoena will harm your investigation, apply for a court order under 18 U.S.C. § 2705(b) to prohibit that disclosure. If you do not inform me within seven days that you have applied for such an order, Ms. Clair will assume that her disclosure of the subpoena will not influence, obstruct, or impede the due administration of justice or otherwise lead to any adverse result in your investigation, and that you have no objection to such disclosure.

The government ultimately never sought a gag order, and never responded to the letter. Therefore, and with the permission of our client Ms. Clair, EFF is now publishing this report about the bogus subpoena so that others might learn from the experience.

So, what lessons have we learned?

6. Closing Lessons

The experience of Ms. Clair in dealing with the subpoena for Indymedia's logs brings with it several lessons — not only for online service providers but also for the average Internet user, Americans who care about civil liberties, and Congress.

The first lesson is for the average Internet user: **yes, your IP address can be and typically is logged by the online services that you use, and yes, the government can obtain those logs,** sometimes with only a subpoena issued directly by a prosecutor. If you want to anonymize your IP address to prevent the violation of your online privacy, you can use anonymizing software such as "Tor". You can find out more about Tor and how it works in this section of EFF's Surveillance Self-Defense Manual and at www.torproject.org.

For online service providers, the second lesson is straightforward, and one that EFF has highlighted both in its "Best Practices for Online Service Providers" and its Surveillance Self-Defense manual: **if you don't have it, they can't get it.** When providers avoid keeping unnecessary Internet logs, responding to subpoenas and other legal demands for such information becomes very simple: "Sorry, but we don't keep those logs and so we don't have any information that's responsive to this subpoena."

The third lesson, again for providers, is that **they can and should seek legal advice when they receive legal demands for information.** Without a lawyer's advice, providers may hand over data that the government isn't legally entitled to or that the provider is legally forbidden from disclosing, and may be cowed into silence by bogus gag demands.

For example, assume that the subpoena in this case had been served on a service that did keep logs of site visitors' IP addresses. Without advice from counsel like EFF, the recipient would not have known that the request, purportedly based on the SCA, actually violated the SCA, and that providing the information to the government could have created liability for the service provider.

Nor would the provider have understood that the subpoena's purported requirement of secrecy was actually an unenforceable request, or that if there was a gag order it could be challenged in court on First Amendment grounds. Absent advice from a lawyer, the provider's unquestioning silence would unnecessarily add to the growing fog of secrecy that surrounds the government's practices in this area.

This leads to our fourth and final lesson, for members of Congress and their constituents: **the level of secrecy surrounding how the government uses its surveillance authority under the Stored Communications Act encourages abuses.** Sunlight is the best disinfectant, and the best protection against such abuses is more clarity and transparency when it comes to how the SCA is used. Americans who care about civil liberties should press Congress to update the SCA to further clarify what it does and does not authorize, and to require detailed public reporting about how the statute is used, just like the federal wiretap statute requires annual reports on law enforcement's wiretapping activities. Without such reform, we may never know how often the government issues unlawful demands like the one described here, or how often providers secretly comply with those demands. The government must be held accountable for its uses — and abuses — of its surveillance authority, and with your and Congress' help, it can be held to account.

Until that day, EFF continues to stand ready to provide assistance the next time the government knocks on someone's door with an unlawful, invalid, overbroad, free speech-threatening, privacy-invasive demand for

your sensitive Internet data.

Legal Disclaimer

This report is for informational purposes only and does not constitute legal advice. if you have any specific legal problems, issues, or questions, please do not act on this legal information alone. Seek a complete review of your situation with a lawyer licensed to practice in your jurisdiction, as different factual situations and different legal jurisdictions may lead to different results.

Want to learn how you can defend free speech, stand up for privacy, fight for government transparency, support consumer rights, and protect your right to innovation in the digital world? Visit **http://eff.org/fight** to find ways to help.