# AN EPIC EFFORT TO COMBAT THE DRAGNET

The Electronic Privacy Information Center has filed a writ of mandamus to SCOTUS to overturn the Section 215 order turning over all of Verizon's call records to the NSA.

Let me be clear: this is a moon shot. I'm doubtful it'll work. A really helpful post at SCOTUSblog on the effort emphasizes how unusual this is.

> EPIC's move is the boldest of a number of legal challenges to NSA that have been filed around the country by privacy defenders in the wake of Snowden's public disclosure of some of the details of NSA surveillance. EPIC filed under a Supreme Court rule that permits "extraordinary" filings directly in the Supreme Court, without first making a trip through a lower court, when "exceptional circumstances warrant the exercise of the Court's discretionary powers" and an adequate remedy cannot be obtained "from any other court." The history of such Rule 20 requests shows that few are granted. The Court's own rules say that the power to grant such pleas is "sparingly exercised."

All that said, IMO the filing is very well crafted, and worth reading with attention.

**Name check the key Justices**

I first got sucked in by the way the introduction invokes two recent cases on these issues.

> The records acquired by the NSA under this Order detail the daily activities, interactions, personal and business relationships, religious and political affiliations, and other intimate details

> of millions of Americans. “Awareness that the Government may be watching chills associational and expressive freedoms. And the Government’s unrestrained power to assemble data that reveal private aspects of identity is susceptible to abuse.” United States v. Jones, 132 S. Ct. 945, 956 (2012) (Sotomayor, J., concurring). As Justice Breyer has recently noted, “the Government has the capacity to conduct electronic surveillance of the kind at issue.” Clapper v. Amnesty Int’l, USA, 133 S.Ct. 1138, 1158- 59 (2013) (citing, inter alia, Priest & Arkin, A Hidden World, Growing Beyond Control, Wash. Post, July 19, 2010, at A1 (reporting that the NSA collects 1.7 billion e-mails, telephone calls and other types of communications daily)). And because the NSA sweeps up judicial and Congressional communications, it inappropriately arrogates exceptional power to the Executive Branch.

Sotomayor is the one Justice who “gets” the implications of this dragnet; her opinion in Jones summarized where an ideal SCOTUS would be on these issues. If this is going to work Sotomayor is going to need to hold the hands of the other Justices and walk them through this risk. And Breyer is a key swing, a vote likely to support law and order without a good argument to the contrary.

And notice the way EPIC slipped in the separation of powers argument right there?

The motion also name checks two more crucial Justices, Republicans who have supported civil liberties issues on key cases in the past. Most importantly, it invokes Scalia’s recent warning against a panopticon in Maryland v. King (the DNA case).

> Even admirable ends do not justify the creation of a panopticon. See Maryland

> v. King, 569 U.S. __, 133 S.Ct. 1958, 1989 (2013) (Scalia, J., dissenting) ("Solving unsolved crimes is a noble objective, but it occupies a lower place in the American pantheon of noble objectives than the protection of our people from suspicionless lawenforcement searches.").

It uses Alito (who wrote the governing opinion in US v. Jones) to validate David Kris' work on national security investigations and its emphasis that this is supposed to be about foreign intelligence.

> As Justice Alito recently stated for the Court in Clapper:
>
> > Congress enacted the Foreign Intelligence Surveillance Act (FISA) to authorize and regulate certain governmental electronic surveillance of communications for foreign intelligence purposes. See 92 Stat. 1783, 50 U.S.C. § 1801 et seq.; 1 D. Kris & J. Wilson, National Security Investigations & Prosecutions §§ 3.1, 3.7 (2d ed. 2012) (hereinafter Kris & Wilson). [. . .] In FISA, Congress authorized judges of the Foreign Intelligence Surveillance Court (FISC) to approve electronic surveillance for foreign intelligence purposes if there is probable cause to believe that "the target of the electronic surveillance is a foreign power or an agent of a foreign power," and that each of the specific "facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power."

And threw in a paper Alito wrote years ago,

anticipating a FISA Court, for good luck (though I'm curious whether and how this citation actually helps this argument).

> The need for a statute and a court to oversee national security surveillance was anticipated several years before enactment of the FISA and the establishment of the FISC. See Report of the Chairman – Samuel Alito, Conference on the Boundaries of Privacy in American Society, Woodrow Wilson Sch. of Pub. & Int'l Affairs, Princeton Univ. at 5 (Jan. 4, 1972).

**There are no other courts that can hear this petition**

After appealing to those four key Justices, the brief then makes the case to justify the mandamus petition. EPIC has to come to SCOTUS, it argues, because the rules of FISC prevent it from petitioning there.

> The FISC and Foreign Intelligence Surveillance Court of Review ("Court of Review") only have jurisdiction to hear petitions by the Government or recipient of the FISC Order, and neither party to the order represents EPIC's interests. Other federal courts have no jurisdiction over the FISC, and thus cannot grant the relief that EPIC seeks.

And no other court has jurisdiction over Section 215 orders.

> Only this Court, the Court of Review, and the FISC are empowered to consider petitions to affirm, modify, or set aside a FISA Business Records order. 50 U.S.C. § 1861(f)(3). As a result, EPIC cannot petition an inferior federal court to vacate the unlawful FISC Order.

This is part of the genius of their demand here

– asking only to overturn the Verizon order approved in April. That's because it limits the possible jurisdiction to FISC and its appellate courts, which gives you a way to get to SCOTUS directly.

Furthermore, as SCOTUSblog reported, it ultimately presents a fairly narrow question.

> Marc Rotenberg, EPIC's president, told reporters that the organization had kept its request narrow, to reflect the significance of the unusual plea it was asking the Court to consider. "It would have been a little bit too much," he said, if EPIC had sought some immediate action by the Court, or if it had added a constitutional question, such as the impact of the Fourth Amendment's privacy guarantees. The case as filed, he said, is focused solely on whether the federal law has been "appropriately applied."
>
> Noting that he has had extensive experience in privacy cases, Rotenberg commented that "I've never seen a court order as broad – applied solely to domestic communications."
>
> Asked to discuss the potential impact on this petition of the Court's Clapper decision, he said there were "key facts" making the two cases difference: first, that the Clapper case involved a surveillance program of unknown scope, while the petition relies upon the actual text of Judge Vinson's order showing its breadth, and, second, that much of the Clapper ruling was focused on gathering foreign intelligence, while this case involves communications in the U.S.

**FISC has exceeded its authority**

Which gets us to the other part of qualifying their mandamus petition. The FISC, EPIC argues, has overstepped their mandate.

> The ongoing collection of the domestic telephone records of millions of Americans by the NSA, untethered to any particular investigation, is beyond the authority granted by Congress to the FISC under the FISA. Because of the structure of the FISA and the FISC, EPIC can only obtain relief from this Court.

There are three interesting claims here. First, FISC has rendered the limiting phrase "relevant" utterly meaningless.

> What makes a tangible thing "relevant" to an authorized investigation is likewise not clearly delineated in the statute. However, in accordance with the foreign intelligence purposes of FISA, the Act says that tangible things are "presumptively relevant" if they
>
>> pertain to – (i) a foreign power or an agent of a foreign power; (ii) the activities of a suspected agent of a foreign power who is the subject of such authorized investigation; or (iii) an individual in contact with, or known to, a suspected agent of a foreign power who is the subject of such authorized investigation[.]
>
> 50 U.S.C. § 1861(b)(2)(A). Common sense dictates that the vast majority of Verizon's customers will not fall into any of these three categories. Consequently, the vast majority of the telephone records conveyed to the NSA will not be presumptively relevant. The burden is therefore on the FBI to show, with specific and articulable facts, why those records are in fact relevant and should be included in the production order.
>
> Moreover, the scope of the request cannot simply encompass all call records

> in the database. To define the scope of the records sought as "everything" nullifies the relevance limitation in the statute. If law enforcement has "everything," there will always be some subset of "everything" that is relevant to something.

Ya think?

In addition, FISC's approval of this order does not comply with Executive Order 12,333's requirement that intelligence collection directed as US persons use the "least intrusive" means possible.

> Executive Order 12,333 requires intelligence agencies to "use the least intrusive collection techniques feasible within the United States or directed at U.S. persons abroad." Id. at § 2.4. The unbounded collection and review of the call detail records of all Americans is plainly not "the least intrusive technique feasible."

Clearly collecting everybody's phone data does not qualify as least intrusive.

Finally, EPIC brings up something I noted this morning: There's a FISC statute authorizing phone record collection — the Pen Register/Trap and Trace — and that's not what the government is using.

> Use of pen registers and trap and trace devices is the classic technique that this Court has recognized for the collection of call detail records, which were originally simply telephone numbers dialed. See Smith v. Maryland, 442 U.S. 735 (1979). Pen registers and trap and trace devices are also used for present and future monitoring of communications, as opposed to historical record collection. They are the sorts of devices and methods one would use to

> capture telephony metadata. To the extent that Congress intended to allow the FISC to order ongoing domestic communications surveillance for foreign intelligence purposes, such orders should be rooted in section 1842 concerning pen registers and trap and trace devices, not section 1861's tangible things provisions.

Since the Verizon order was disclosed, I've been wracking my brains to understand why they used Section 215 rather than Section 1842. I still don't understand it. But hopefully it proves problematic here.

**Contrary to government claims, US identities are at stake**

EPIC then uses several of the materials released by the Guardian to argue against something Administration figures have long been claiming: this is not, in fact, anonymized collection.

> The FISC Order also compels disclosure of personally identifiable information. Telephone numbers, IMSI numbers, and IMEI numbers are unique and can be used to identify individuals. The NSA maintains a database of "telephone numbers and electronic communications accounts / addresses / identifiers that NSA has reason to believe are being used by United States Persons." Procedures used by the Nat'l Sec. Agency for Targeting Non-U.S. Persons Reasonably Believed to be Located Outside the U.S. to Acquire Foreign Intelligence Info. Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, As Amended, Nat'l Sec. Agency, at 3 (FISA Ct. filed Jul. 29, 2009). 18 These numbers collected under the FISC Order can be easily matched with the records maintained in the NSA identifying database. **In fact, the NSA uses this matching process to "prevent the**

> **inadvertent targeting of a United States person" under directives issued pursuant to Section 702 of FISA. Id.**
>
> **Because telephone numbers identify individuals, they are protected as personal information under federal law.** See, e.g., 15 U.S.C. § 6501(8)(A)-(E) (2012) (including "telephone number" within the definition of personal information); 18 U.S.C. § 2725(3) (2012), (including "telephone number" within the definition of personal information). See also 47 U.S.C. § 222(h)(1)(A) (2012) (defining "customer proprietary network information" as "information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service. . . .").
>
> The telephony metadata obtained under the FISC Order is used by the NSA to create maps of an individual's social connections. These social maps contain information about users private contacts and associations. This process is referred to as "contact chaining," and it is used to structure and catalog the telephony metadata held by the NSA. See Memorandum from Kenneth Wainstein, Assistant Att'y Gen., Dep't of Justice, to the Att'y Gen. of the United States, at 2 (Nov. 20, 2007). 19 Contact chaining allows the agency to "automatically identify not only the first tier of contacts made by the seed telephone number or e-mail address, but also the further contacts made by the first tier of telephone numbers or e-mail addresses and so on." Id. at 13. So if the NSA was investigating Bob's telephone records, and saw he called Jane, the NSA would then collect and examine all of Jane's telephone records. If they saw that Jane called Steve, they

> would then collect and examine all of Steve's telephone records. Contact chaining was specifically designed as a means to analyze the communications metadata of U.S. persons. Id. at 2. 20 But this process also gives rise to combinatorial explosion, permitting the creation of enormous data sets containing personal information completed unrelated to the purpose of the investigation. [my emphasis]

After laying out one of the better technical arguments for the problem with the metadata program as reflected in the totality fo the documents released so far, EPIC throws in Joe:

> The practical use of telephone numbers to identify individuals is well understood. In 2006, Senator Joe Biden told CBS News that "I don't have to listen to your phone calls to know what you're doing. If I know every single phone call you made, I'm able to determine every single person you talked to. I can get a pattern about your life that is very, very intrusive."

**Courts have have used mandamus to prevent similar harms in the past**

Finally EPIC lays out a number of harms that courts have used to prevent in the past. The first ties to EPIC personally: its ability to protect attorney client privilege on issues it litigates against the US.

> At present, EPIC is in litigation with both the NSA and FBI, the two agencies responsible for tracking Americans' private communications under this order. EPIC v. FBI, No. 13-442 (D.D.C. 2013); EPIC v. FBI, No. 12-667 (D.D.C. 2012); EPIC v. NSA, No. 10-196 (D.D.C. 2010). Additionally, EPIC has ongoing FOIA lawsuits against other elements of the

> Intelligence Community, including the Office of the Director of National Intelligence and the Central Intelligence Agency. EPIC v. ODNI, No. 12-1282 (D.D.C. 2012); EPIC v. CIA, 12-2053 (D.D.C. 2012). At the FISC's command, Verizon is turning over EPIC's privileged information to the very parties capable of exploiting that information.22 The court's order hampers EPIC's ability to deliberate and develop litigation strategies "free from the consequences or the apprehension of disclosure." Hunt v. Blackburn, 128 U.S. 464, 470 (1888). See also Weatherford v. Bursey, 429 U.S. 545, 554 n.4 (1977) (noting that government surveillance of attorneyclient communications threatens the "inhibition of free exchanges between defendant and counsel."). //Courts consider a threat to attorney-client communications an exceptional circumstance and have issued writs of mandamus to vacate production orders implicating privileged information. See, e.g., In re BankAmerica Corp. Sec. Litig., 270 F.3d 639 (8th Cir. 2001) (attorney-client); Admiral Ins. Co. v. U.S. Dist. Court for the Dist. of Ariz., 881 F.2d 1486 (9th Cir. 1989) (attorney-client); In re Fink, 876 F.2d 84 (11th Cir. 1989) (doctor-patient).

EPIC then goes on to cite another harm relating to its mission: several cases that granted mandamus to protect the speech of advocacy groups.

Finally, it drops the hammer that even the Senate Appropriations Committee was bothered about until the NSA told them they purge certain data in secret (and the one harm listed in that introduction): such collection violates separation of powers.

> The FISC Order threatens the autonomy of the Legislative and Judicial branches by

> authorizing the Executive to collect the telephone communication records of Members of Congress and federal judges. The Framers determined that the creation of three coequal branches of government was "essential to the preservation of liberty." Mistretta v. United States, 488 U.S. 361, 380 (1989). Accordingly, the Constitution prohibits efforts by one branch to control, interfere with, or unduly burden the exercise of the constitutionally assigned functions of another branch.
>
> [snip]
>
> This interference with the communicative freedom of members of the judiciary and legislature "impair[s these branches] in the performance of [their] constitutional duties," Clinton v. Jones, 520 U.S. 681, 701 (1997), and thereby threatens the separation of powers. Thus, mandamus is warranted to remedy the interference.

Ultimately, it's a two-fold argument: one appealing to the Justices own well-developed sense of turf (not to mention the Republicans' disapproval of institutions that exceed their mandate). But nested within that, what I consider a well-argued case for the harms involved in this program.

It probably won't work, but who knows? I read somewhere SCOTUS, like much of the rest of official DC, uses Verizon.