# Ex Post CP

## NEGATIVE

### 1nc – generic

#### Text: The United States federal government should require ex post review by the Foreign Intelligence Surveillance Court of \_\_\_\_\_\_\_\_\_ (NSA domestic surveillance OR unpiloted aerial vehicles domestic surveillance OR FBI domestic profiling) targeting criteria. The United States federal government should also establish a public advocate at the FISC.

#### Solvency: The CP restores confidence in US without restricting the scope of surveillance activities – instead it conducts post-surveillance minimization of the impacts.

Margulies ‘14 **-** Professor of Law, Roger Williams University School of Law (“CITIZENSHIP, IMMIGRATION, AND NATIONAL SECURITY AFTER 9/11: THE NSA IN GLOBAL PERSPECTIVE: SURVEILLANCE, HUMAN RIGHTS, AND INTERNATIONAL COUNTERTERRORISM” 82 Fordham L. Rev. 2137, April, lexis)

While I have concluded that U.S. surveillance policy does not violate the ICCPR, further reforms could highlight this point and silence persistent doubts here and abroad. These reforms could also remove any barriers to cooperation between the United States and foreign states, such as those in Europe, which are subject to the European Convention on Human Rights. This section identifies reforms that would add a public advocate to FISC proceedings, enhance FISC review of the criteria used for overseas surveillance, establish a U.S. privacy agency that would handle complaints from individuals here and overseas, and require greater minimization of non-U.S. person communications. These reforms would signal U.S. support of evolving global norms of digital privacy. Although President Obama's speech in January 2014 proposed a panel of independent lawyers who could participate in important FISC cases, n161 further institutionalization of this role would be useful. A public advocate would scrutinize and, when necessary, challenge the NSA's targeting criteria on a regular basis. n162 Challenges would be brought in the FISC, after the NSA's implementation of criteria. The NSA would be able to adapt the criteria on an exigent basis, subject to ex post review by the FISC at the public advocate's behest. A public advocate and enhanced FISC review would serve three valuable functions: (1) ensure that the FISC received the best arguments on both sides; (2) serve as a valuable ex ante check on the government, encouraging the government to adopt those criteria that could withstand subsequent scrutiny; and (3) promote domestic and global confidence in the legitimacy of processes governing NSA surveillance.

#### The net benefit is terrorism – the CP solves but avoids the chilling effect of ex ante restrictions that prevents the government from reacting in exigent circumstances

Margulies ‘14 [Peter, Professor of Law, Dynamic Surveillance: Evolving Procedures in Metadata and Foreign Content Collection After Snowden, <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2400809&download=yes>] Schloss

The better course for Congress would be to offer an itemized, but not exhaustive list of permissible uses of U.S. person identifiers. Congress could permit U.S. person queries in cases involving pre-existing FISA orders, threats to life, efforts to join international terrorist groups (the ISIS example), and other transnational illegal activity. This list would not categorically bar other uses of U.S. person identifiers, allowing some room for those uses when compelling circumstances arose. However, it would frame the substantive discussion in a useful way, and send a signal to the FISC and the executive branch that deliberation on the scope of U.S. person queries was vital. A set of guidelines like those suggested would also compensate for the broader latitude that the NSA has for incidental collection under § 702. In cases that comprise the basis for the incidental collection doctrine, a federal judge had already issued a warrant based on probable cause to believe that wrongdoing had occurred.383 That is not the case with § 702, where the FISC merely reviews government targeting procedures.384 The latitude permitted under § 702 gives the government more room to frame initial searches to ensnare Americans. Critics have surely exaggerated the government’s ability to engage in reverse targeting. Evidence that the NSA has engaged in such practices is slim to nonexistent. However, a dynamic approach that adjusts to the post-Snowden climate should not treat the absence of reported abuse as a recipe for complacency. Instead, this is the appropriate time to put in place safeguards that will avoid abuse in the future. External constraints should be optimal for providing flexibility while ensuring checks on potential abuse. As in other situations, a public advocate should receive notice of the NSA’s use of U.S. person identifiers to query § 702 data. Once a statutory standard is in place, the advocate should be able to seek FISC review of any identifier when a reasonable possibility exists that the use of the identifier does not comply with Congress’s formulation. This review would be ex post, to avoid chilling the agency’s discretion in exigent situations. Ex post review would still be meaningful, given the NSA’s status as a repeat player dependent on the FISC’s continued good will. External constraints of this kind would assure critics that substantive standards were being followed. This external check is essential in the post-Snowden climate, in which internal “protocols” have – perhaps to a fault – become objects of corrosive cynicism.

### 2nc – NSA specific

#### Ex post oversight is key to effective programmatic surveillance – the CP allows the government to collect all available data – it just puts ex post restrictions on the data analysis stage that deters executive data abuses

**Sales, 14** - Associate Professor of Law, Syracuse University College of Law (Nathan, I/S: A Journal of Law and Policy for the Information Society, “Domesticating Programmatic Surveillance: Some Thoughts on the NSA Controversy” 10 ISJLP 523, Summer, lexis)

As for the operational considerations, among the most important is the need for external checks on programmatic surveillance. In particular, bulk data collection should have to undergo some form of judicial review, such as by the FISA court, in which the government demonstrates that it meets the applicable constitutional and statutory standards. Ideally, the judiciary would give its approval before collection begins. But this will not always be possible, in which case timely post-collection judicial review will have to suffice. (FISA has a comparable mechanism for temporary warrantless surveillance in emergency situations.) n60 Programmatic surveillance also should be subject to robust congressional oversight. This could take a variety of forms, including informal consultations with members of Congress when designing the surveillance regime (including, at a minimum, congressional leadership and members of the applicable committees), [\*537] as well as regular briefings to appropriate personnel on the operation of the system and periodic oversight hearings. Of course, judicial review in the context of bulk collection won't necessarily look the same as it does in the familiar setting of individualized monitoring of specific targets. If investigators want to examine the telephony metadata associated with a particular terrorism suspect, they can apply to the FISA court for a pen register or trap and trace order upon a showing that the information sought is relevant to an ongoing national security investigation. n61 But, as explained above, that kind of particularized showing often won't be possible where authorities are dealing with unknown threats, and where the very purpose of the surveillance is to identify those threats. In these situations, reviewing courts may find it necessary to allow the government to collect large amounts of data without individualized suspicion. This doesn't mean that privacy safeguards must be abandoned and the executive given free rein. Instead, courts could be tasked with scrutinizing the initiative's overall structure and operation to determine its compatibility with constitutional and statutory requirements. And courts further could require authorities to demonstrate some level of individualized suspicion before accessing the data that has been collected. Protections for privacy and civil liberties thus can migrate from the collection phase of the intelligence cycle to earlier and later stages, such as the systems design and analysis stages. n62 In more general terms, because programmatic surveillance involves the collection of large troves of data, it likely means some dilution of the familiar ex ante restrictions that protect privacy by constraining the government from acquiring information in the first place. It therefore becomes critically important to devise meaningful ex post safeguards that can achieve similar forms of privacy protection. In short, restrictions on the government's ability to access and use data that it has gathered must substitute for restrictions on the government's ability to gather that data at all; what I have elsewhere called use limits must stand in for collection limits. n63 This sort of oversight by the courts and Congress provides an obvious, first-order level of protection for privacy and civil liberties--an external veto serves as a direct check on possible executive [\*538] misconduct. Judicial and legislative checks also offer an important second-order form of protection. The mere possibility of an outsider's veto can have a chilling effect on executive misconduct, discouraging officials from questionable activities that would have to undergo, and might not survive, external review. n64 Moreover, external checks can channel the executive's scarce resources into truly important surveillance and away from relatively unimportant monitoring. This is so because oversight increases the administrative costs of collecting bulk data--e.g., preparing a surveillance application, persuading the judiciary to approve it, briefing the courts and Congress about how the program has been implemented, and so on. These increased costs encourage the executive to prioritize collection that is expected to yield truly valuable intelligence and, conversely, to forego collection that is expected to produce information of lesser value.

### 2nc – Drones specific

#### An ex-post review of drone strikes solves the aff, makes FISA review more effective, and avoids the link to the terror DA

Hafetz, 13 - Associate Professor of Law, Seton Hall University School of Law (Jonathan, “Reviewing Drones” 3/08/13, http://www.huffingtonpost.com/jonathan-hafetz/reviewing-drones\_b\_2815671.html)//jml

Pre-strike review, moreover, would place judges in the untenable position of having to sign death warrants -- a position judges are likely to resist. Judges, to be sure, make rulings every day with enormous consequences for human life and liberty. But they typically do so only after a trial, where both sides have presented evidence, and not -- as in the case of the FISA court -- in a secret proceeding based solely on the government's evidence. A FISA review model would, in short, risk legitimizing drone strikes without providing any real check on their use. The better course is to ensure meaningful review after the fact. To this end, Congress should authorize federal damages suits by the immediate family members of individuals killed in drone strikes. Such ex post review would serve two main functions: providing judicial scrutiny of the underlying legal basis for targeted killings and affording victims a remedy. It would also give judges more leeway to evaluate the facts without fear that an error on their part might leave a dangerous terrorist at large. For review to be meaningful, judges must not be restricted to deciding whether there is enough evidence in a particular case, as they would likely be under a FISA model. They must also be able to examine the government's legal arguments and, to paraphrase the great Supreme Court chief justice John Marshall, "to say what the law is" on targeted killings. Judicial review through a civil action can achieve that goal. It can thus help resolve the difficult questions raised by the Justice Department white paper, including the permissible scope of the armed conflict with al Qaeda and the legality of the government's broad definition of an "imminent" threat. Judges must also be able to afford a remedy to victims. Mistakes happen and, as a recent report by Columbia Law School and the Center for Civilians in Conflict suggests, they happen more than the U.S. government wants to acknowledge. Errors are not merely devastating for family members and their communities. They also increase radicalization in the affected region and beyond. Drone strikes -- if unchecked -- could ultimately create more terrorists than they eliminate. Courts should thus be able to review lethal strikes to determine whether they are consistent with the Constitution and with the 2001 Authorization for Use of Military Force, which requires that such uses of force be consistent with the international laws of war. If a drone strike satisfies these requirements, the suit should be dismissed. Government officials, moreover, would be liable only if they violate clearly established legal standards. This limitation helps avoid chilling the use of drones where the law is uncertain, while still deterring their misuse. Critics will contend that civil suits would mark an unprecedented intrusion into executive decision-making. But in recognizing the right of enemy combatants to seek judicial review of their detention through habeas corpus, the Supreme Court has made clear that even a state of war is not a blank check for the president. It misses the essential teaching of these rulings to insist that courts can review the government's decision to deprive a person of his liberty, but not his life.

#### Ex post review allows effective oversight without hindering drone effectiveness

Taylor, 13 – Senior Research Fellow Center for Policy & Research at Seton Hall University School of Law (Paul, February 9, A FISC for Drones? http://transparentpolicy.org/2013/02/a-fisc-for-drones/)//jml

However, many of the suggestions for a tribunal to review these killings call instead for ex post review. This is the model required in Israel. The basic idea of this is generally that waiting until the operation is complete keeps the court out of the way of military or para-military operations, but still maintains some oversight. Robert Chesney of Lawfare provided some very interesting points to consider about such a court, including whether the review should be ex ante or ex post. He falls on the side of ex ante, but some of his commentary actually seems to point in the other direction. First, he points out the all of the serious propositions would subject the nomination process to judicial review, not the “trigger pull.” This temporally removes the judicial authorization from the final decision to kill, and in Chesney’s view eliminates the concern that the process will interfere with the execution of the operation. I’m not sure that it does. Names may be placed on the list at any time, conceivably as the result of a time sensitive push within the intelligence community. While I am not an expert in the process of targeting decisions, I think that the executive may need to be able to act quickly on new information that indicates that a subject is targetable. Ex ante review would place an additional hurdle between the decisive intelligence and the operation. Chesney seems to realize this by admitting the need for an “exigent circumstances exemption.” But this exception would itself mean defaulting back to an ex post review. Additionally, Chesney notes that “Some judges want absolutely nothing to do with this … due to hostility to the idea of judicial involvement in death warrants. (And that’s without considering the possibility of warrant-issuing judges finding themselves the object of suit or prosecution abroad.)” Judges would likely be much more comfortable with ex post review. Ex post review would free them from any implication that they are issuing a “death warrant” and would place them in a position that they are much more comfortable with: reviewing executive uses of force after the fact. While there are clearly parallels that could be drawn between the ex ante review proposed here and the search and seizure warrants that judges routinely deal with, there are also important differences. First and foremost is that this implicates not the executive’s law enforcement responsibility but its war-making and foreign relations responsibilities, with which courts are loath to interfere, but are sometimes willing to review for abuse. Additionally, in search and seizure warranting, there an ex post review will eventually be available. That will likely not be the case in drone strikes and other targeted killings unless such a process is specifically created. There are simply too many hurdles to judicial review (including state secrets, political questions, discovery problems, etc) for the courts to create such an opportunity without congressional action. Chesney also noted that executive officials involved in the nomination process would prefer an ex ante review to shield them from unexpected civil liability by the victims or their families. I’m sure that it is true that administration officials would like to have “certainty ex ante that they would not face a lawsuit.” However, this is not a guarantee that the courts can provide to the executive. As noted above, as with search and seizure warrants, there are issues to consider after the approval of the executive action. Ex ante review does not allow for inquiry into important ancillary issues, such as the balancing of risk to civilian bystanders. Also, it provides no assurances that new, exculpatory intelligence forces a reassessment of the targeting decision. Only ex post review would achieve this.

### 2nc – Ex Post solves

#### The CP’s ex post review process deters executive abuse and restores legitimacy to US surveillance

**Sales, 14** - Associate Professor of Law, Syracuse University College of Law (Nathan, I/S: A Journal of Law and Policy for the Information Society, “Domesticating Programmatic Surveillance: Some Thoughts on the NSA Controversy” 10 ISJLP 523, Summer, lexis)

As for the structural considerations, one of the most important is what might be called an anti-unilateralism principle. A system of programmatic surveillance should not be put into effect on the say-so of the executive branch, but rather should be a collaborative effort that involves Congress (in the form of authorizing legislation) or the judiciary (in the form of FISA court review of the initiatives). n42 An example of the former is FISA itself, which Congress enacted in 1978. At the time, the NSA was engaged in bulk collection, without judicial approval, of certain international communications into and out of the United States--namely, by tapping into offshore telecommunications cables and by eavesdropping on satellite based radio signals. FISA's [\*533] famously convoluted definition of "electronic surveillance" n43 preserved these preexisting practices even as Congress was imposing a new requirement of judicial approval for other kinds of monitoring. n44 An example of the latter concerns the warrantless Terrorist Surveillance Program, under which the NSA was intercepting, outside the FISA framework, certain communications between suspected al-Qaeda figures overseas and people located in the United States. After that program's existence was revealed in late 2005, the executive branch persuaded the FISA court to issue orders allowing it to proceed subject to various limits. n45 (That accommodation eventually proved unworkable, and the executive then worked with Congress to put the program on a more solid legislative footing through the temporary Protect America Act of 2007 n46 and the permanent FISA Amendments Act of 2008.) n47 Anti-unilateralism is important for several reasons. To take the most obvious, Congress and the courts can help prevent executive overreach. n48 The risk of abuse is lessened if the executive branch must enlist its partners before commencing a new surveillance initiative. Congress might decline to permit bulk collection in circumstances where it concludes that ordinary, individualized monitoring would suffice, or it might authorize programmatic surveillance subject to various privacy protections. In addition, inviting many voices to the decision-making table increases the probability of sound outcomes. More participants with diverse perspectives can also help mitigate the groupthink tendencies to which the executive branch is sometimes [\*534] subject. n49 If we're going to engage in programmatic surveillance, it should be the result of give and take among all three branches of the federal government, or at least between its two political branches, not the result of executive edict. A second principle follows from the first: Programmatic surveillance should, wherever possible, have explicit statutory authorization. Congress does not "hide elephants in mouseholes," n50 the saying goes, and we should not presume that Congress meant to conceal its approval of a potentially controversial programmatic surveillance system in the penumbrae and interstices of obscure federal statutes. Instead, Congress normally should use express and specific legislation when it wants to okay bulk data collection. Clear laws will help remove any doubt about the authorized scope of the approved surveillance, thereby promoting legal certainty. Express congressional backing also helps give the monitoring an air of legitimacy. And, a requirement that programmatic surveillance usually should be approved by clear legislation helps promote accountability by minimizing the risk of congressional shirking. n51 If the political winds shift, and a legislatively approved program becomes unpopular, Congress will not be able to hide behind an ambiguous statutory grant of power and deflect responsibility to the President.

#### Ex ante review undermines effective restrictions on domestic surveillance and shuts down an engaged citizenry

**Harvard Law Review, 8** – no author cited, “SHIFTING THE FISA PARADIGM: PROTECTING CIVIL LIBERTIES BY ELIMINATING EX ANTE JUDICIAL APPROVAL” http://cdn.harvardlawreview.org/wp-content/uploads/pdfs/shifting\_the\_FISA\_paradigm.pdf

Ex ante judicial review is not only of limited effectiveness, but it is also affirmatively harmful in several respects. Ex ante judicial approval imparts a broader imprimatur of validity than is warranted given the limited effectiveness of the review. Further, it clouds accountability and can be a cumbersome and intrusive process harmful to national security interests. In fact, “the creation of FISA courts may actually have resulted in fewer restrictions on the domestic surveillance activities of intelligence agencies”69 because “[t]he secrecy that attends FISC proceedings, and the limitations imposed on judicial review of FISA surveillance, may insulate unconstitutional surveillance from any effective sanction.”70 1. The Judicial Imprimatur. — The issuance of an order by the FISC confers a stamp of approval from the widely respected Article III courts. A FISC order makes a strong statement that a neutral arbiter has looked closely at the situation and found the surveillance warranted. Yet, as the set of limitations just discussed indicates, the protective force of a FISC order may not align with the actual vigor of the inquiry. This disparity may give rise to several problems. First, changed circumstances following the issuance of the order may undermine the validity of the surveillance. Minimization procedures are largely unhelpful in solving this problem: “[T]he Act provides for the same kind of incoherent and largely unenforceable ‘minimization’ requirements that plague criminal wiretap statutes.”71 Much more importantly, the judicial order may mask and indeed later provide cover for improper governmental motives and improper intrusions on liberty.72 In these situations, ex ante review may sanitize the improper surveillance. The presence of the judicial order may function to dissuade legislative or executive oversight entities from inquiry. Worse, judicial orders offer the potential for the government to hide behind the nominally objective, even if only minimally rigorous, scrutiny that they represent. Surveillance conducted for political reasons, for example, might escape detection, condemnation, and consequences — political, if not legal — if that surveillance is given judicial protection.73 Indeed, this sanitization could occur on an even broader level: ex ante judicial approval interferes with the healthy public skepticism that attends political actors and that may help keep the citizenry engaged in considering the difficult tradeoffs between liberty and security necessary in this context. This is not to say that the judiciary should decline to play a constitutionally permissible role; rather, the point is that system designers concerned with protecting civil liberties should keep in mind the drawbacks of ex ante approval. In total, the capacity of ex ante approval to enable some of the most dangerous sorts of abuses far outweighs its middling ability to provide a useful check.

### AT: Courts will defer

#### Ex post review creates executive self-restraint despite deference

**Goitein and Patel 15** - Elizabeth (Liza) Goitein co-directs the Brennan Center for Justice’s Liberty and National Security Program. Served as counsel to Sen. Russell Feingold with a particular focus on government secrecy and privacy rights. Was a trial attorney in the Federal Programs Branch of the Civil Division of the Department of Justice. Graduated from the Yale Law School and clerked for the Honorable Michael Daly Hawkins on the U.S. Court of Appeals for the Ninth Circuit. Faiza Patel serves as co-director of the Brennan Center for Justice’s Liberty and National Security Program. Clerked for Judge Sidhwa at the International Criminal Tribunal for the former Yugoslavia. Ms. Patel is a graduate of Harvard College and the NYU School of Law. (Elizabeth and Faiza, “What went wrong with the FISA court”, Brennan Center for Justice at New York University School of Law, 2015 //DM)

290 Advocates for greater oversight might argue that a clear error review — on a matter in which the judiciary already is inclined to be deferential to the executive’s judgments — would accomplish little. In fact, however, the requirement would serve an important checking function. By forcing the government to articulate the factual basis for choosing selectors, it would create an incentive for self-restraint at the front end of the process. While it is unlikely that the FISA Court would reject any of the selectors that the government submitted to it, it is quite likely that the list of selectors presented to the court would be smaller and better justified than would otherwise be the case. On the flip side, the government would no doubt argue that this proposal represents an unworkable burden on the executive branch and the FISA Court. If the government’s scope of collection remained as broad as it is now, that argument might hold some weight. However, the burden stemming from this proposal should be greatly diminished by the reinstatement of the “agent of a foreign power” and “primary purpose” criteria, as well as the narrowing of the definition of “foreign intelligence information.” Following these changes, the number of targets for whom selection terms must be presented to the court — while no doubt large — should be nowhere near the reported 89,000 targets today. 2013 Transparency Report, supra note 178 (estimating that 89,138 targets were affected by Section 702 in 2013).

### AT: FISC oversight weak

#### The public advocate part of the CP and the strengthening of PCLOB to make it a cabinet level agency remedies existing weaknesses of the FISC

**Setty, 15** - Professor of Law and Associate Dean for Faculty Development & Intellectual Life, Western New England University School of Law (Sudha, “Surveillance, Secrecy, and the Search for Meaningful Accountability” 51 Stan. J Int'l L. 69, Winter, lexis)

One promising move with regard to oversight and transparency has been the establishment and staffing of the Privacy and Civil Liberties Oversight Board (PCLOB). n186 This board, tasked with assessing many aspects of the government's national security apparatus both for efficacy and for potentially unnecessary incursions into civil liberties, has a broad mandate and, compared with many national security decision makers, significant independence from the executive branch. n187 Retrospectively, the PCLOB has, among other things, issued the highly critical report of the NSA Metadata Program in January 2014 that led to further public pressure on the Obama administration to curtail this program; it is promising that the PCLOB's prospective agenda includes further analysis of various surveillance programs. n188 However, the PCLOB's potential influence in protecting civil rights may be limited by its position: The PCLOB is an advisory body that analyzes existing and proposed programs and possibly recommends changes, but it cannot mandate that those changes be implemented. The ability to have a high level of access to information surrounding counterterrorism surveillance programs and to recommend changes in such programs is important and should be lauded, but over-reliance on the PCLOB's non-binding advice to the intelligence community to somehow solve the accountability and transparency gap with regard to these programs would be a mistake. For example, on prospective matters, it is likely that intelligence agencies would consult the PCLOB only if the agency itself considers the issue being faced new or novel, as the NSA metadata program was labeled prior to its inception. In such cases, decision makers within an agency generally ask whether the contemplated program is useful or necessary, technologically feasible, and legal. If all three questions are answered affirmatively, the program can be implemented. Now that the PCLOB is fully operational, it seems likely that if a contemplated program is considered new or novel, an intelligence agency would consult the PCLOB at some stage of this process for its guidance on implementing the program. This nonpartisan external input may improve self-policing within the [\*102] intelligence community and help intelligence agencies avoid implementing controversial programs or, even if implemented, set better parameters around new programs. n189 If the PCLOB is able to exert some degree of soft power in influencing national security decision-making, then the judiciary represents hard power that could be used to force the protection of civil liberties where it might not otherwise occur. The FISC should be reformed to include a public advocate lobbying on behalf of privacy concerns, making the process genuinely adversarial and strengthening the FISC against charges that it merely rubber stamps applications from the intelligence community. n190 Article III courts need to follow the lead of Judge Leon in Klayman in conceptualizing privacy as broad and defensible, even in a world where electronics-based communication is dominant and relatively easy for the government to collect. If the judicial defense of privacy were combined with the possibility of liability for violations of that privacy, it is likely that this would incentivize increased self-policing among the members of the intelligence community. The creation of an active PCLOB and a more adversarial process before the FISC will not provide a perfect solution to the dilemmas posed by the government's legitimate need for secrecy and the protection of the public against potential abuse. Yet because these changes are institutional and structural, they are well-placed to improve the dynamic between the intelligence community, oversight mechanisms, and the public. Conclusion Genuine accountability should not depend on the chance that an unauthorized and illegal leak will occur. In the comparative example of the United Kingdom, engagement with a European Union energized with a commitment to increase privacy protections, along with domestic parliamentary oversight, provide two potential avenues for increased constraint on surveillance. In India, the parliament and the courts historically enabled, not constrained, the intelligence community. Whether that stance will continue as the government's technological capabilities increase is yet to be seen. Domestically, it could be argued that the types of reform recommended here to improve actual accountability and transparency over programs like the NSA Metadata Program are overkill: They involve multiple branches of government, the PCLOB, and the public. However, much of the accountability apparatus that has been in place was dormant until the Snowden disclosures, and would have remained passive without those disclosures. A multi-faceted, long-term, structural approach [\*103] to improving transparency and accountability - one that involves at a minimum the courts and the PCLOB, but hopefully Congress, the executive branch, and the public as well - improves the likelihood of sustained and meaningful accountability as new surveillance capabilities are developed and implemented.

### 2nc – FISC special advocate solves

#### A public advocate would check FISC rubber stamping

**Cetina 14**– John Marshall Law School (Daniel, “Balancing Security and Privacy in 21st century America: A Framework for FISA Court Reform”, John Marshall Law Review, Summer 2014, <http://heinonline.org/HOL/Page?collection=journals&handle=hein.journals/jmlr47&type=Text&id=1540)//DBI>

The first remedy involves appointing a privacy advocate whose sole duty would be to argue against the government's warrant requests, in essence acting as a quasi-public defender or guardian of privacy rights.' 0 ' Such an idea is already percolating in the House of Representatives.102 Retired Judge James Robertson, who formerly presided over the FISA Court, claims this is a necessary step 0 3 because the Court has frequently been merely a proverbial rubber stamp for surveillance requests.104 Indeed, available literature suggests that the FISA Court grants over 90% of the government's requests. 105 Introducing a privacy advocate would effectively force the FISA Court to consider individual requests from both perspectives: on the one hand, the government would present important security arguments, while the privacy advocate would focus on potential or actual dangers to cognizable privacy interests. This system would thereby promote equity in FISA Court proceedings and enable the public at large to have a representative promote privacy.

#### A public advocate would be easy to implement and would reform much of the single-mindedness of the past FISC decisions

Schlanger 15 [Margo, Professor of Law at the University of Michigan Law School, and the founder and director of the Civil Rights Litigation Clearinghouse., Intelligence Legalism and the National Security Agency’s Civil Liberties Gap, [file:///C:/Users/Jonah/Downloads/Intelligence%20Legalism%20and%20the%20National%20Security%20Agency-s%20Civil%20Li%20(2).pdf](file:///C%3A/Users/Jonah/Downloads/Intelligence%20Legalism%20and%20the%20National%20Security%20Agency-s%20Civil%20Li%20%282%29.pdf)] Schloss3

Finally, it seems highly likely that in the near future, the FISA Court will gain a new process for occasional appearance of a public or special advocate. This proposal has been endorsed in varying forms by the Director of National Intelligence,393 the President’s Review Group,394 the PCLOB,3 and the President.396 It was included in the recently-defeated Senate’s USA FREEDOM Act bill, which will be one source for the next Congress’s work on the issue. 397 Even former FISA presiding Judge John Bates, now the Director of the Administrative Office of the U.S. Courts, agrees in part.398 There is, however, substantial disagreement about details—and the details matter. The argument for such an advocate is straightforward: even if the government exhibits exemplary candor as to facts, it cannot be relied upon to brief against its own authority. Because the issues are complex and important, they deserve full adversarial development in support of better judicial decision-making. The arguments against are likewise easily summarized: There’s not enough for a special advocate to do, since most issues before the FISA Court are not legally complex, and the facts will not be available to the advocate. Adversarial process will be slower and more cumbersome without leading to better decision-making. Indeed, it might lead to worse decision-making, because “adversarial process in run-of-the-mill, fact-driven cases may erode” the government’s compliance with a “heightened duty of candor to the Court.”399 Indeed, “intelligence agencies may become reluctant to voluntarily provide to the Court highly sensitive information, or information detrimental to a case, because doing so would also disclose that information to a permanent bureaucratic adversary.”400 The consensus for some form of public advocate does not encompass key details. The largest open question is about access. Under the House version of the USA Freedom Act, FISA court public advocates could have been excluded from factual or even legal presentations by the government to FISA judges and their legal advisors.401 The Senate version of the bill, by contrast, specified that public advocates would receive “access to all relevant legal precedent, and any application, certification, petition, motion, or such other materials as are relevant to the duties of the special advocate.”402 Judge Bates, who served for six years as a FISA Court judge, has written several letters to Congress,403 purportedly on behalf of the judiciary,404 opposing a full-time, autonomous special advocate in the FISA Court. Those letters pointed out, as a disadvantage, that inclusion of adversarial process would make the FISA Court more court-like. Judge Bates explained that “FISC judges currently have substantial flexibility in deciding how best to receive from the government information they consider relevant to a particular case.” That flexibility, he suggested, could not survive inter partes procedural requirements: In order for the FISC to abide by the procedural and ethical requirements that apply in adversarial proceedings, and for the advocate to appear on equal footing with the applicant, the FISC would have to ensure that the advocate was involved in all such interactions in any case in which the advocate may participate. . . .We expect that the logistical challenges of administering such a three-way process for more than a handful of cases would be considerable.405 The Obama Administration, unfortunately, seems to be favoring limiting access, as well: In a letter to Senator Pat Leahy about the Senate bill, Attorney General Eric Holder and Director of National Intelligence James Clapper opined that “the appointment of an amicus in selected cases…need not interfere with…the process of ex parte [that is, one-party] consultation between the Court and the government.”406 In fact, the FISA court and the public would be best served by a more empowered public advocate—one who is authorized to appear even without invitation from the government or the court, and, still more important, who is entitled to full access to information relevant to her duties. This would no doubt alter the current one-party procedures before the FISA court. But that’s a feature, not a bug. The FISA Court’s current procedures allow meetings quite unlike ordinary judicial hearings, even ex parte ones. In advance advice from court staff to the government and iterative drafting are common. The 2009 PowerPoint slide deck already described is similarly odd for a judicial forum.”407 Other practices such as an annual lunch bringing together FISA Court judges and legal advisors (and the Chief Justice) with the heads of the CIA, NSA, and FBI likewise encourage the judges to see their own role as co-workers in the administration of the intelligence community’s surveillance programs, supervising, for sure, but almost from within. If a public advocate’s procedural rights disrupted this cozy relationship, that would be all to the good. The salutary effect might be to reinforce the FISA judges’ role as arbiters of surveillance legality, not coworkers in the administration of the IC’s surveillance programs. If designed properly, this variation of an Office of Goodness could be essentially free from the ordinary threats to that kind of organization’s influence and commitment. After all, the role of government-paid court opponent is utterly familiar from the criminal justice system. Unlike agencies, where staff must negotiate for a seat at decision-making tables, most courts have firm inter partes norms requiring access for all parties.408 If Congress applies these norms to the FISA court, as it should, implementation will be very familiar. As for capture, the analogous public defenders certainly sometimes allow organizational or situational imperatives to subvert their assigned courtroom role, 409 but there seems far less reason to worry about capture in this litigation setting than inside of agencies, at least if the public advocates are not otherwise beholden to the agencies. If anything, the problem here might be too much single-minded commitment, a strict preference for civil liberties over security—but of course the court, which would remain the decider, is unlikely to become unduly single-minded. I therefore see a FISA Court public advocate as a variant on an Office of Goodness whose institutional setting would—if it is well designed—shield it from many of the landmines that usually threaten such an office’s influence or commitment.

### AT: Special advocate links to terrorism

#### The special advocate functions ex post – ex ante advocacy compromises terrorism investigations

Vladeck 15 – Professor of Law at American University Washington College of Law (Stephen, THE CASE FOR A FISA “SPECIAL ADVOCATE,” 2 Texas A&M L. Rev. 2)//JJ

To be sure, Judge Bates is certainly correct that the participation of the special advocate should not unduly interfere with the government’s ability to conduct lawful foreign intelligence surveillance activities, especially ex ante. To that end, the special advocate might only be notified of a government application under the relevant authorities once that application has been granted by FISC, at which time the appointed advocate would have a fixed period of time within which to seek reconsideration of the underlying ruling. Among other things, this approach would allow the government to act expeditiously when circumstances warrant (lest an expressly legislated emergency exception otherwise swallow the rule), and would preserve the status quo (in which authorization has been provided by the FISC) until and unless the special advocate convinces the FISC judge, the FISCR, or the Supreme Court to vacate such authorization. And, of course, if the special advocate prevails before either the FISC or FISCR, the government retains the option of seeking a stay of the ruling in question to continue the underlying surveillance pending appeal.

### 2nc – terrorism net-benefit

#### FISA’s authority alone is insufficient to prevent terrorism – the government needs the widest possible net, including domestic surveillance

**Posner, 6** - judge on the United States Court of Appeals for the Seventh Circuit in Chicago and a Senior Lecturer at the University of Chicago Law School (Richard, Not a Suicide Pact: The Constitution in Time of National Emergency, p. 94-96

According to the administration, these are just interceptions of communications to and from the United States in which one of the parties is suspected of terrorist connections, though the suspicion does not rise to the probable-cause level that would be required for obtaining a warrant. There may be more to the program, however. Most likely the next terrorist attack on the United States will, like the last one, be mounted from within the country but be orchestrated by leaders safely ensconced somewhere abroad. If a phone number in the United States is discovered to have been called by a known or suspected terrorist abroad, or if the number is found in the possession of a suspected terrorist or in a terrorist hideout, it would be prudent to intercept all calls, domestic as well as international, to or from that U.S. phone number and scrutinize them for suspicious content. But the mere fact that a suspected or even known terrorist has had a phone conversation with someone in the United States or has someone’s U.S. phone number in his possession doesn’t create probable cause to believe that the other person is also a terrorist; probably most phone conversations of terrorists are with people who are not themselves terrorists. The government can’t get a FISA warrant just to find out whether someone is a terrorist; it has to already have a reason to believe he’s one. Nor can it conduct surveillance of terrorist suspects who are not believed to have any foreign connections, because such surveillance would not yield *foreign* intelligence information. FISA has yet another gap. A terrorist who wants to send a message can type it in his laptop and place it, unsent, in an e-mail account, which the intended recipient of the message can access by knowing the account name. The message itself is not communicated. Rather, it’s as if the recipient had visited the sender and searched his laptop. The government, if it intercepted the e-mail from the intended recipient to the account of the “sender,” could not get a FISA warrant to intercept (by e-mailing the same account) the “communication” consisting of the message residing in the sender’s computer, because that message had never left the computer. These examples suggest that surveillance outside the narrow bounds of FISA might significantly enhance national security. At a minimum, such surveillance might cause our foreign terrorist enemies to abandon or greatly curtail their use of telephone, e-mail, and other means of communicating electronically with people in the United States who may be members of terrorist sleeper cells. Civil libertarians believe that this is bound to be the effect of electronic surveillance, and argue that therefore such surveillance is futile. There is no “therefore.” If the effect of electronic surveillance is to close down the enemy’s electronic communications, that is a boon to us because it is far more difficult for terrorist leaders to orchestrate an attack on the United States by sending messages into the country by means of couriers. But what is far more likely is that some terrorists will continue communicating electronically, either through carelessness— the Madrid and London bombers were prolific users of electronic communications, and think of all the drug gangsters who are nailed by wiretaps—or in the mistaken belief that by using code words or electronic encryption they can thwart the NSA. (If they can, the program is a flop and will be abandoned.) There are careless people in every organization. If al-Qaeda is the exception, civil libertarians clearly are underestimating the terrorist menace! In all our previous wars, beginning with the Civil War, when telegraphic communications were intercepted, our enemies have known that we might intercept their communications, yet they have gone on communicating and we have gone on intercepting. As for surveillance of purely domestic communications, it would either isolate members of terrorist cells (which might, as I said, have no foreign links at all) from each other or yield potentially valuable information about the cells. FISA’s limitations are borrowed from law enforcement. When a crime is committed, the authorities usually have a lot of information right off the bat—time, place, victims, maybe suspects—and this permits a focused investigation that has a high probability of eventuating in an arrest. Not so with national security intelligence, where the investigator has no time, place, or victim and may have scant idea of the enemy’s identity and location; hence the need for the wider, finer-meshed investigative net. It is no surprise that there have been leaks from inside the FBI expressing skepticism about the NSA program. This skepticism reflects the Bureau’s emphasis on criminal investigations, which are narrowly focused and usually fruitful, whereas intelligence is a search for the needle in the haystack. FBI agents don’t like being asked to chase down clues gleaned from the NSA’s interceptions; 999 out of 1,000 turn out to lead nowhere. They don’t realize that often the most that counterterrorist intelligence can hope to achieve is to impose costs on enemies of the nation (as by catching and “turning” some, or forcing them to use less efficient means of communication) in the hope of disrupting their plans. It is mistaken to think electronic surveillance a failure if it doesn’t intercept a message giving the time and place of the next attack.

#### FISA can’t identify unknown terrorists – advance surveillance is necessary to generate enough information

**Sales, 14** - Associate Professor of Law, Syracuse University College of Law (Nathan, I/S: A Journal of Law and Policy for the Information Society, “Domesticating Programmatic Surveillance: Some Thoughts on the NSA Controversy” 10 ISJLP 523, Summer, lexis)

Programmatic surveillance thus can help remedy some of the difficulties that arise when monitoring covert adversaries like international terrorists. FISA and other particularized surveillance tools are useful when authorities want to monitor targets whose identities are already known. But they are less useful when authorities are trying to identify unknown targets. The problem arises because, in order to obtain a wiretap order from the FISA court, the government usually must demonstrate probable cause to believe that the target is a foreign power or agent of a foreign power. n39 This is a fairly straightforward task when the target's identity is already known--e.g., a diplomat at the Soviet embassy in Washington, DC. But the task is considerably more difficult when the government's reason for surveillance is to detect targets who are presently unknown--e.g., al-Qaeda members who operate in the shadows. How can you convince the FISA court that Smith is an agent of a foreign power when you know nothing about Smith--his name, nationality, date of birth, location, or even whether he is a single person or several dozen? The government typically won't know those things unless it has collected some information about Smith--such as by surveilling him. And there's the rub. Programmatic monitoring helps avoid the crippling Catch-22 that can arise under particularized surveillance regimes like FISA: officials can't surveil unless they show that the target is a spy or terrorist, but sometimes they can't show that an unknown target is a spy or terrorist unless they have surveilled him.

### AT: Perm do both

#### The permutation increases the burden on the government and inhibits investigations

**Kerr, 10 -** Professor, George Washington University Law School (Orin, “EX ANTE REGULATION OF COMPUTER SEARCH AND SEIZURE” Virginia Law Review, October, SSRN)

At the same time, all of the ex ante restrictions will necessarily be poor proxies for an ex post review of reasonableness. Instead of substituting for ex post review of reasonableness, ex ante restrictions supplement those restrictions. Ex ante limitations force the government to follow two sources of law: the reasonableness of executing the warrant imposed by reviewing courts ex post, and the restrictions imposed by the magistrate judge ex ante. If the ex ante restrictions happen to be modest, or are drafted in a way that ensures that they are always less than or equal to the restrictions of reasonableness ex post, then such restrictions will merely replicate the ex post reasonableness determinations. But every time an ex ante restriction goes beyond ex post reasonableness, the restrictions will end up prohibiting the government from doing that which is constitutionally reasonable. The limitations will be unreasonable limitations caused by judicial error.

#### Ex ante restrictions are highly error prone

**Kerr, 10 -** Professor, George Washington University Law School (Orin, “EX ANTE REGULATION OF COMPUTER SEARCH AND SEIZURE” Virginia Law Review, October, SSRN)

Ex ante restrictions tend to introduce constitutional errors in this environment. To be sure, such restrictions stem from the best of intentions: they reflect a good-faith effort to identify what will be constitutionally reasonable.201 However, ex ante predictions of reasonableness will be more error prone than ex post assessments for two major reasons. First, ex ante restrictions require courts to “slosh [their] way through the factbound morass of reasonableness” 202 without actual facts. Second, ex ante restrictions are imposed in ex parte hearings without legal briefing or a hearing. Both reasons suggest that ex ante restrictions often will inaccurately gauge the reasonableness of how warrants are executed. The major difficulty with ex ante restrictions is that the reasonableness of executing a warrant is highly factbound, and judges trying to impose ex ante restrictions generally will not know the facts needed to make an accurate judgment of reasonableness. Granted, magistrate judges might have a ballpark sense of the facts, from which they might derive a sense of what practices are ideal. For example, they might think that it is unreasonable to seize all of a suspect’s home computers if on-site review is possible. Alternatively, they might think it is unreasonable to conduct a search for image files if the warrant only seeks data not likely to be stored as an image. They might think it is unreasonable to keep a suspect’s computer for a very long period of time without searching it. All of these senses will be based on a rough concept of how the competing interests of law enforcement and privacy play out in typical computer searches and seizures. At the same time, these ballpark senses of reasonableness can never improve past very rough approximation. A magistrate judge cannot get a sense of the exigencies that will unfold at each stage of the search process. The reasonableness of searching on-site will not be known until the agents arrive and determine how many computers are present, what operating systems they use, and how much memory they store. The needed time window before the government searches the seized computer depends on how much the government can prioritize that case over other cases, given existing forensic expertise and resources, as well as which agency happens to be working that case.203 The reasonableness of different search protocols depends on the operating systems, an analyst’s expertise in forensics, which forensics programs the government has in its possession, what kind of evidence the government is searching for, and whether the suspect has taken any steps to hide it.204 Finally, the reasonableness of retaining seized computers that have already been searched depends on whether the government might need the original computer as evidence or whether it ends up containing contraband that should not be returned and is subject to civil forfeiture. 205 The magistrate presented with an application for a warrant simply cannot know these things. Judges are smart people, but they do not have crystal balls that let them predict the number and type of computers a suspect may have, the law enforcement priority of that particular case, the forensic expertise and toolkit of the examiner who will work on that case, whether the suspect has tried to hide evidence, and if so, how well, and what evidence or contraband the seized computers may contain. Magistrate judges can make ballpark guesses about these questions based on vague senses of what happens in typical cases. But even assuming they take the time to learn about the latest in law enforcement resources and the computer forensics process—enough to know about typical cases—they cannot do more than come up with general rules that they think are useful for those typical cases. The errors of ex ante restrictions are particularly likely to occur because warrant applications are ex parte. The investigators go to the judge with an affidavit and a proposed warrant.206 The judge reads over the materials submitted. The judge can modify the warrant, but his primary decision is whether to sign or reject it. The entire process takes a matter of minutes from start to finish. No hearing occurs. There is no testimony beyond the affidavit in most cases, and the affidavit usually contains only standard language about computer searches.207 A prosecutor may be present, but need not be. Obviously, no representative of the suspect is present to offer witnesses or argument. In that setting, judges are particularly poorly equipped to assess reasonableness. The most they can develop is a standard set of ex ante restrictions that they use in all computer warrants, perhaps one shared with other magistrate judges in their district. More careful scrutiny is both impractical and unlikely. The ability of a magistrate judge to assess reasonableness in that setting is a far cry from her ability to rule on reasonableness in an ex post hearing, in which agents and experts can take the stand and counsel for the defendant can cross-examine the agent, offer his own witnesses, submit written briefs, and present oral argument.

## AFF ANSWERS

### AT: Ex Post CP

#### State secrets doctrine means it’s impossible to determine the basis of a FISA warrant ex post

Harper 14, University of Chicago Law School, U.S. Department of Justice, Civil Division, (Nick, “FISA’s Fuzzy Line between Domestic and International Terrorism”, University of Chicago Law Review; Summer2014, Vol. 81 Issue 3)//AK

Unfortunately, the following cases cannot definitively prove whether FISA currently operates as the enacting Congress intended. Such knowledge is shielded from the public by several procedural requirements that kick in when the government decides to prosecute an alleged international terrorist using evidence derived from FISA surveillance. These procedures make it possible for the government to push FISA’s targeting language past its limits and make discovery of such abuse especially difficult. This potential for abuse makes even an imperfect inquiry into the government’s compliance all the more necessary. First, the bases for the vast majority of FISA warrants are never reviewed after they receive FISC approval because of FISA’s unique notice procedures. FISA requires the government to provide notice to a target of surveillance only when the government seeks to use information “obtained or derived from” FISA surveillance in an adversarial proceeding.101 The majority of FISA wiretaps never result in criminal prosecution and are therefore never reviewed by a district court.102 Once the government does decide to prosecute based on evidence derived from FISA surveillance, it invites scrutiny of its probable cause finding by a district court judge. However, if the government expansively interprets FISA’s internationality requirement, it can avoid such oversight when it never uncovers a subsequent international connection—the cases most likely to receive the greatest ex post scrutiny—simply by exercising its prosecutorial discretion. Second, even when the government does prosecute based on FISA-derived evidence, the barriers to discovery of FISA warrant applications make it difficult to ascertain the government’s basis for initiating FISA surveillance. Once a defendant files a motion to disclose the FISA application, FISA permits the government to submit an affidavit from the attorney general stating that “disclosure or an adversary hearing would harm the national security of the United States.”103 Needless to say, the government presents this affidavit in response to every motion to disclose or suppress.104 And once the government submits that affidavit, the district court judge can require disclosure only when “such disclosure is necessary to make an accurate determination of the legality of the surveillance.”105 At the time of this writing, only one court has ever deemed it necessary to require disclosure of FISA application materials, and then only because the defendant’s counsel had top secret security clearance.106 Moreover, that court was later reversed by the Seventh Circuit.107 One major problem with this practice is that the facts that constitute probable cause are never made public. This makes it very difficult for district court judges (and defendants) to evaluate whether the government has established a sufficient international connection. Furthermore, because the government almost never has to reveal FISA applications, it is difficult for the defendant to even argue that probable cause did not exist because ~~he~~ does not know when the surveillance started.108 While the district court judge does see the application, his or her estimation of probable cause could be affected by hindsight bias in cases in which sufficient international links are exposed as a result of the surveillance. This is especially likely to occur considering that only the government is given the opportunity to present arguments to the judge with the full set of facts.

#### Ex post review alone fails – courts lack institutional expertise to review surveillance risks

**Harvard Law Review, 8** – no author cited, “SHIFTING THE FISA PARADIGM: PROTECTING CIVIL LIBERTIES BY ELIMINATING EX ANTE JUDICIAL APPROVAL” http://cdn.harvardlawreview.org/wp-content/uploads/pdfs/shifting\_the\_FISA\_paradigm.pdf

2. Judicially Ordered Notice to Wrongfully Surveilled Persons. — Another approach would provide a stronger statutory cause of action for improper surveillance, adding an ex post review function to the FISC. Such a scheme would “provide compensation to individuals subject to the most grievous instances of unlawful electronic surveillance” by giving the FISC power to “screen for these violations and discretionarily notify an individual,” and then compensate him or her if appropriate.82 This approach is commendable for attempting to remedy the lack of adversariality and the fact that improper surveillance that occurs after a FISC order is issued — when either changed circumstances or invalid governmental motives never come to light because the government does not attempt criminal prosecution — may go unchecked.83 But the suggested remedy, to broaden notice by making a “distinction . . . between disclosure that concretely threatens national security and disclosure that would merely embarrass the government,” 84 seems unworkable. Such line drawing necessarily involves crucial policy determinations that the courts are in a bad institutional position to make. Moreover, the ability of the remedy to provide a check on the government seems at best dubious and could even be viewed as permitting the government to purchase the ability to invade constitutional liberties.

#### Ex post is impossible to enforce and amounts to a rubber stamp

**Berman, 14** - Visiting Assistant Professor of Law, Brooklyn Law School (Emily Berman, Regulating Domestic Intelligence Collection, 71 Wash. & Lee L. Rev. 3,

<http://scholarlycommons.law.wlu.edu/wlulr/vol71/iss1/5>

The suggestion that the FISC approximate the role of traditional judicial review of agency decision making to impose constraints on discretion will also fail to result in the preservation of civil liberties. As an initial matter, it is unclear what the extent of the FISC’s review might be. Traditional judicial review of administrative rules asks whether an agency’s action is consistent with the Constitution and its statutory mandate or whether it is arbitrary or capricious.319 But when it comes to most intelligence-collection rules, there is no constitutional or statutory standard against which a court could measure agency compliance.320 One proposed solution to this baseline problem is to have the FISC review policy for whether it is consistent with the intelligence agencies’ own stated objectives.321 Again, this proposal fails to account for the fact that when the intelligence community is left to determine the rules of its own conduct, concerns other than security will get short shrift. By asking intelligence agencies to identify their own objectives and then subjecting their efforts to meet those objectives to judicial review would replicate the current situation—where the constraints on agencies are limited to those that they agree to place on themselves—but with the added legitimating feature of judicial imprimatur. Another barrier to enlisting the FISC in intelligencecollection governance is that the intelligence-collection activities governed by the Guidelines extend beyond the scope of the FISC’s jurisdiction. The FISC oversees electronic foreign intelligence surveillance and physical searches of premises connected with foreign powers.322 It has no role in overseeing purely domestic surveillance of Americans absent probable cause that those Americans are agents of a foreign power.323 The content of the Guidelines and the activities they regulate—such as physical surveillance of Americans, infiltration of religious or political groups, the use of informants, requests for internet history— rarely fall within the FISC’s jurisdiction. Individuals who wish to challenge FBI activity—if they can establish standing—do not have access to the FISC.324 Thus, it is unclear what role the FISC could play in reviewing many activities in which the FBI engages. The FISC, too, is likely to share the FBI and ODNI’s bias toward the security mission. Unless a recipient of a FISC order challenges the legitimacy of that order, proceedings in the FISC are not subject to an adversarial process.325 Instead, like magistrate judges considering whether to issue traditional search warrants, FISC judges review unopposed government applications for surveillance orders.326 The FISC thus receives only the Justice Department’s perspective—heavily informed by the FBI’s perspective—about any given rule. This concern is compounded by the fact that even the judges themselves largely hail from the law enforcement community—twelve of the fourteen judges who have served this year are former prosecutors and one is a former state police director.327 Moreover, once selected by the Chief Justice of the Supreme Court for FISC service, these judges are exposed to a constant stream of government applications to engage in foreign intelligence collection detailing just how dangerous the world can be and the important role that intelligence collection plays in combating those dangers.328 FISC involvement thus serves only to reinforce the pro-security perspective already embedded in the development of domesticintelligence- collection policies.

#### Secrecy makes meaningful ex post review impossible

**Setty, 15** - Professor of Law and Associate Dean for Faculty Development & Intellectual Life, Western New England University School of Law (Sudha, “Surveillance, Secrecy, and the Search for Meaningful Accountability” 51 Stan. J Int'l L. 69, Winter, lexis)

The extent of congressional knowledge regarding the NSA Metadata Program is not fully known to the public and has been the subject of significant debate. Nonetheless, even assuming that Congress was sufficiently informed as to the potential reach of the PATRIOT Act with regard to surveillance n59 and, therefore, that the statutory authority for the bulk data collection and storage was sound, the ability of Congress to effect significant and meaningful ex post oversight appears to be severely limited. Historically, congressional hearings and investigations have been a powerful tool to rein in executive branch overreaching. n60 However, it seems that the extreme secrecy surrounding the NSA surveillance programs undermined the efficacy of these oversight powers, to the point that they may have been reduced to an ersatz form of accountability. One prominent example stems from a Senate oversight hearing on March 12, 2013, in which Senator Ron Wyden specifically asked Director of National Intelligence James Clapper if the NSA was systematically gathering information on the communications of millions of Americans. n61 Clapper denied this, yet subsequent revelations confirmed that the broad scope of the data collection included metadata for telephonic communications, as well as content data for emails, texts, and other such writings. n62 After public discussion of the discrepancy in his testimony, Clapper commented that he gave the "least most untruthful" answer possible under the circumstances. n63 Senator Wyden expressed disappointment and frustration that even while under oath at an oversight hearing, Clapper misled the Senate. n64 The ability for congressional oversight is further hampered by a general lack of access to information about the details of the NSA Metadata Program n65 and [\*82] lack of ability to discuss publicly whatever knowledge is shared with Congress. n66 In fact, it remains unclear whether senators, including Dianne Feinstein, Chair of the Senate Intelligence Committee, knew of the lapses in NSA procedure until after such information was leaked to news sources. n67 Further revelations indicate that administration statements made to Congress even after the Snowden disclosures were not entirely accurate. n68 These examples are not determinative, but taken together, they raise significant doubt to the extent of accurate information regarding surveillance programs being made available to congressional oversight committees, and whether the oversight committees can function as effective accountability measures n69 without the benefit of illegally leaked information such as the Snowden disclosures.

#### FISC review only has a weak effect on executive deterrence

**Setty, 15** - Professor of Law and Associate Dean for Faculty Development & Intellectual Life, Western New England University School of Law (Sudha, “Surveillance, Secrecy, and the Search for Meaningful Accountability” 51 Stan. J Int'l L. 69, Winter, lexis)

The FISC differs from Article III courts in numerous ways: Its statutory scope is limited to matters of foreign intelligence gathering; its judges are appointed in the sole discretion of the Chief Justice of the United States Supreme Court; its proceedings are secret; its opinions are often secret or are published in heavily [\*83] redacted form; and its process is not adversarial as only government lawyers make arguments defending the legality of the surveillance being contemplated. n70 Many of these differences bring into doubt the legitimacy of the court, its ability to afford adequate due process regarding civil liberties concerns, and its ability to uphold the rule of law in terms of government accountability. Compounding this legitimacy deficit is the FISC's own loosening of the relevance standard under Section 215 of the PATRIOT Act such that the FISC has found that bulk data collection without any particularized threat or connection to terrorism is legally permissible. n71 Historically, the FISC has rejected NSA surveillance applications too infrequently to be considered a substantial check on government overreach as an ex ante matter. n72 As an ex post matter, it is unclear to what extent the FISC's work guarantees any meaningful accountability over NSA surveillance activities. On the one hand, because the FISC lacks an adversarial process and has no independent investigatory authority, the FISC only addresses ex post compliance problems when the government itself brings the problem to the court's attention. n73 As such, FISC judges rely on the statements of the government as to the government's own behavior and lack the authority to investigate the veracity of the government's representations. n74 For example, in 2011, the FISC found one aspect of the surveillance program - brought to its attention months after the program went into effect n75 - to be unconstitutional. n76 Additionally, in one declassified opinion, the FISC critiques the NSA's sloppy over-collection of metadata of U.S. communications, and questions the efficacy of bulk data collection as a national security measure. n77 At one point, the FISC sanctioned the NSA for overreaching in [\*84] saving all metadata and running daily metadata against an "alert list" of approximately 17,800 phone numbers, only 10% of which had met FISC's legal standard for reasonable suspicion. n78 On such occasions, the administration has modified problematic aspects of the surveillance and continued forward without further impediment by the FISC. n79 On the other hand, the fact that the NSA itself has brought potential compliance incidents to the notice of the FISC n80 indicates at least some internal policing of these programs. However, this is hardly an effective substitute for external review and accountability mechanisms that would ensure that consistent controls are in place. Further, the self-reporting of these compliance incidents does not in any way allow for discourse over the larger structural questions surrounding the surveillance programs. Finally, the ability of the FISC to act as an effective check on NSA overreaching is severely limited by the secrecy and lack of information available to the FISC judges. Judge Reggie B. Walton, formerly the Chief Judge of the FISC, lamented that "the FISC is forced to rely upon the accuracy of the information that is provided to the Court ... . The FISC does not have the capacity to investigate issues of noncompliance ... ." n81 The ability of the NSA to not only gather and retain bulk metadata, but also to build in backdoor access into data files despite private encryption efforts has been largely sanctioned by the FISC based on NSA representations as to the seriousness of the security threats posed to the nation. n82 In an environment in which there is a tremendous fear of being held responsible for any future terrorist attack that might occur on U.S. soil, n83 and in which there is a [\*85] information deficit for those outside of the intelligence community, the FISC has consistently deferred to the NSA's assertions and has not been able to act as an effective accountability mechanism.

#### Ex post fails – hindsight bias and secrecy

**Morgan, 8** - Law Clerk to the Honorable Samuel H. Mays, Jr., United States District Court for the Western District of Tennessee. J.D., 2007, New York University School of Law (Alexander, “A BROADENED VIEW OF PRIVACY AS A CHECK AGAINST GOVERNMENT ACCESS TO E-MAIL IN THE UNITED STATES AND THE UNITED KINGDOM” 40 N.Y.U. J. Int'l L. & Pol. 803, Spring, lexis)

Ex post judicial review is compromised by hindsight bias. n192 Strict reliance on ex post approaches presupposes that judges charged with determining the sufficiency of original [\*836] search justifications are capable of ignoring potentially inculpatory evidence since uncovered. As with the notion of a disinterested Home Secretary, this appears at odds with human nature. n193 The delay or outright denial of notice to search targets minimizes the efficacy of judicial review. Without notice, "the majority of interferences with privacy will be undetected," and most will only learn that they were surveillance targets if criminal charges follow. n194 By implication, the true extent of surveillance (and any abuse) remains unknown. n195 Untimely notice also compromises the value of judicial review because the court will be privy to the fruits of a search already conducted and thus susceptible to hindsight bias. In the United Kingdom, the Home Secretary never gives notification, n196 and delayed notice is fast growing in the United States through the use of "sneak and peek" warrants. n197 Gauging the scope of surveillance in the United Kingdom is further frustrated by non-responsive Tribunal decisions which "simply state whether the determination is favourable ... thus, not necessarily revealing [if] there has been any interception or its details." n198 [\*837] Independent monitors such as the Interception of Communications Commissioner are prone to hindsight bias and also suffer from distinct shortcomings due to their generalized function. Their general charge allows them to uncover and address (through recommendations to Parliament) systemic defects more easily, unlike courts, which are limited to case-by-case review. The converse is that monitors lack authority to remedy any specific abuses they uncover. n199 Above all, commentators characterize monitors as helpless because there are too many authorizations to oversee, such that "not all authorisations are subject to scrutiny; only those selected at random." n200 In sum, the government's power to withhold notice precludes targets from seeking judicial review, and the result is that many authorizations are never held "to any form of independent scrutiny." n201

### AT: FISC public advocate

#### A FISA public advocate would just be ignored by the FISC

**Slobogin, 15** – Professor of Psychiatry and Director of Criminal Justice Program at Vanderbilt University (Christopher, “Standing and Covert Surveillance”, Vanderbilt University Law School Public Law and Legal Theory, 18 February 2015,  [Pepperdine Law Review, Forthcoming; Vanderbilt Public Law Research Paper No. 15-5. , http://ssrn.com/abstract=2567070//gg](file:///C%3A%5CUsers%5CDavid%5CDesktop%5Cnsa%20aff%20work%20group%5CPepperdine%20Law%20Review%2C%20Forthcoming%3B%20Vanderbilt%20Public%20Law%20Research%20Paper%20No.%2015-5.%20%2C%20http%3A%5Cssrn.com%5Cabstract%3D2567070%5Cgg)

Other possible mechanisms for challenging the metadata program and related programs are unlikely to pick up the slack. Of course, as it has with communications interceptions, Congress could grant standing (and require the predicate notice) to those criminal defendants who are aggrieved by metadata surveillance.56 But because these programs are even more covert than the Section 702 warrant-based interceptions involved in Clapper—and given the government’s penchant for engaging in “parallel construction”57—the chances of such notice would probably be slim to none.58 Congress could also create a special advocate in the Foreign Intelligence Surveillance Court to represent the interests of those whose information is queried, a procedure endorsed by President Obama’s special commission and included in the administration’s recently proposed legislation.59 But whether such an advocate’s office could be counted on to overcome its governmental provenance and the nonchalance that can come from proceeding in secret to develop into a vigorous advocate for individual constitutional claims is at best unclear.60 Moreover, the advocate’s ability to appeal an adverse decision by the FISC is tenuous.61 **Footnote 60:** 60 The history of similar internal oversight mechanisms does not inspire optimism in this regard. See SIMON CHESTERMAN, ONE NATION UNDER SURVEILLANCE: A NEW SOCIAL CONTRACT TO DEFEND FREEDOM WITHOUT SACRIFICING LIBERTY 80 (2011) (“Secrecy . . . . may facilitate cover-ups, block investigators, or transform overseers into defenders. . . . [T]here are good reasons to be wary of any structure that relies entirely on government actors.”).

#### A FISC public advocate fails – won’t solve cred and the state secrets privilege allows circumvention

**Cetina 14**– John Marshall Law School (Daniel, “Balancing Security and Privacy in 21st century America: A Framework for FISA Court Reform”, John Marshall Law Review, Summer 2014, <http://heinonline.org/HOL/Page?collection=journals&handle=hein.journals/jmlr47&type=Text&id=1540)//DBI>

2. Limitations

These good-faith proposals suffer from numerous flaws. Regarding the first proposal, the ideological composition of the FISA Court and the judiciary's historic deference to the executive in matters of foreign affairs113 - especially as applied to domestic defense 114 - suggest that a privacy advocate would become a token figure without any influence. There is also the critical question of what role a public advocate would actually assume. Indeed, a "permanently constituted advocate seeking injunctive relief based on a violation of law in the interest of the general public might be viewed as engaging in a government function," but "a private party appointed temporarily to litigate on behalf of the public might not be considered" a government agent. 115 This distinction could create Appointment Clause issues.116 Also, the federal government may attempt to circumvent this agent by relying on the state secrets privilege.117 Likewise, the second proposal suffers from problems. First, the FISA Court judges are appointed from existing federal districts;118 hence, Congress has already confirmed them. But since the FISA Court is not a traditional Article III court, 119 what role - if any - the Senate could have in potential confirmations is unclear at best. Second, requiring a supermajority consensus on FISA Court decisions is a manifestly unwise decision considering Congress's - and the country's - increasingly polarized nature. 120 Indeed, absent a supermajority by the sitting president's party, it is highly unlikely Congress could reach such a substantial threshold consensus on FISA Court surveillance decisions.121 The polarization argument applies with equal force to the senatorial confrmation suggestion; such hypothetical confirmation proceedings would arguably be even more rancorous and partisan than regular federal judgeship confirmations 122 given the controversial nature of the FISA Court and the parties' mutual obstreperousness. 123 In short, although the two highlighted proposals present promising prospects, their deficiencies severely blunt their effectiveness. And while some of the proposed remedies may mitigate the established system's problems from a practical perspective, more is needed to realize true reform. The FISA Court, along with lower federal courts considering individual surveillance challenges, requires an articulable substantive remedy that will fairly protect both security interests and privacy interests while also providing judicial stability and a semblance of decisional uniformity.

#### **Special advocate doesn’t solve and undermines FISA**

Bates 14 – United States District Judge for the United States District Court for the District of Columbia, B.A. from Wesleyan University, J.D. from the University of Maryland School of Law (John, Comments of the Judiciary on Proposals Regarding the Foreign Intelligence Surveillance Act, ADMINISTRATIVE OFFICE OF THE UNITED STATES COURTS, 1/10/14, [http://www.judiciary.senate.gov/imo/media/doc/011413RecordSub-Grassley.pdf)//JJ](http://www.judiciary.senate.gov/imo/media/doc/011413RecordSub-Grassley.pdf%29//JJ)

The participation of a privacy advocate is unnecessary and could prove counterproductive in the vast majority of FISA matters, which involve the application of a probable cause or other factual standard to case-specific facts and typically implicate the privacy interests of few persons other than the specific target. Given the nature of FISA proceedings, the participation of an advocate would neither create a truly adversarial process nor constructively assist the Courts in assessing the facts, as the advocate would be unable to communicate with the target or conduct an independent investigation. Advocate involvement in run-of-the-mill FISA matters would substantially hamper the work of the Courts without providing any commensurate benefit in terms of privacy protection or otherwise; indeed, such pervasive participation could actually undermine the Courts' ability to receive complete and accurate information on the matters before them.

In those matters in which an outside voice could be helpful, it is critical that the participation of an advocate be structured in a manner that maximizes assistance to the Courts and minimizes disruption to their work. An advocate appointed at the discretion of the Courts is likely to be helpful, whereas a standing advocate with independent authority to intervene at will could actually be counterproductive.

#### Special advocate fails and increases terror threat

Bates 14 – United States District Judge for the United States District Court for the District of Columbia, B.A. from Wesleyan University, J.D. from the University of Maryland School of Law (John, Comments of the Judiciary on Proposals Regarding the Foreign Intelligence Surveillance Act, ADMINISTRATIVE OFFICE OF THE UNITED STATES COURTS, 1/10/14, [http://www.judiciary.senate.gov/imo/media/doc/011413RecordSub-Grassley.pdf)//JJ](http://www.judiciary.senate.gov/imo/media/doc/011413RecordSub-Grassley.pdf%29//JJ)

In our view, some proposals that have been made - especially those that would create a full-time independent advocate to oppose a wide range of government applications before the Courts - present substantial difficulties that would not be resolved by simply increasing the Courts' resources. We anticipate that this form of advocate participation would not only be cumbersome and resource-intensive, but also would impair the FISC's ability to receive relevant information, thereby degrading the quality of its decisionmaking. We turn first to this question.