VERISIMILITUDE IN NATIONAL SECURITY CASES

*Joel Todoroff**

The presence of classified information makes criminal trials far more difficult, particularly for defendants who may be unable to see the evidence against them. This article does two things. First, it looks at how information is released under the Special Advocate system as well as the Classified Information Procedures Act (CIPA) and the criticisms these systems have faced. Second, it proposes a modified form of releasing information which is intended to increase the strength of the adversarial process without incurring additional security risks. This concept, referred to as source/method modified information, functions on the concept of verisimilitude – the idea that some things may be closer to truth than others. I argue that this can be used in conjunction with existing processes and that its use would be beneficial to defendants, the government, and the public.

* J.D. Candidate, Class of 2014, NYU School of Law.

INTRODUCTION

This is about a minor detail of a relatively unknown judicial process. This is also about terrorism. And stories. This is about the trouble we have bringing terrorists to justice when classified information is at stake, and about lies and counterintelligence and what we want the court to be.

Mohamed, a twenty-eight year old resident of the United Kingdom, found himself in Afghanistan. It was dark in his cell. And loud, always loud. Noises, including the screams of women and children, blared twenty-four hours a day. Mohamed's whole body, including penis, had been cut with a scalpel and a stinging liquid poured into the open wounds. He was deprived of food. His relief was transfer to the Guantanamo Bay military prison.[1] When Mohamed later sued, the court stated, "we are bound to follow the Supreme Court's admonition that 'even the most compelling necessity cannot overcome the claim of privilege if the court is ultimately satisfied that [state] secrets are at stake.' After much deliberation, we reluctantly conclude this is such a case, and the plaintiffs' action must be dismissed."[2]

In *A. v. United Kingdom*,[3] a group of defendants found themselves detained, two accused of fundraising for terrorist organizations and two others for being members of terrorist groups linked to the infamous terror organization, Al Qaeda. The problem was that they were given no real evidence to rebut. The two accused of fundraising were presented with evidence that large sums of money went through their bank accounts but they were never provided with information linking their accounts and terrorists.[4] Those accused of membership were presented with mere allegations thereof.[5]

It's hard to have a trial when classified information is involved. Normally, trials and courts are open, there is transparency and a foundational notion that parties argue on equal footings. Normal procedures of this nature recoil when such practices would compromise national security however. Government intelligence services seek to avoid compromising national security information such as sources or

1. Mohamed v. Jeppesen Dataplan, Inc., 563 F.3d 992, 998 (9th Cir. 2009).

2. Mohamed v. Jeppesen Dataplan, Inc., 614 F.3d 1070, 1073 (9th Cir. 2010) (internal citations omitted). The case alleged that Jeppeson Dataplan, Inc., a United States corporation, was liable for providing logistical support to the intelligence organizations that undertook these activities. The government intervened claiming a trial would implicate state secrets. The court agreed, holding that litigation was simply infeasible without the use of classified information. *See id.* at 1092–93.

3. *See generally* A. v. United Kingdom, App. No. 3455/05, Eur. Ct. H.R. (2009).

4. *Id*. at ¶ 223.

5. *Id*. at ¶ 224.

methods. A fully transparent process would almost inevitably lead to such a compromise. The bind is that without relatively complete information it is difficult to mount an effective defense. The accused may not be able to engage with the evidence against them and, as a result, appear guilty despite their innocence.

Countries have created various mechanisms to deal with this complication, ranging from modifying criminal trials to limiting judicial review entirely. A large number of western liberal democracies focus on modifying normal criminal procedure to accommodate classified information. One common way to do this is to allow only certain lawyers access to the classified information, ensuring that national security information is not compromised but retaining some degree of protection for the suspect as the lawyer can argue on their behalf. A potential complication is that in these situations the suspect may be unable to see the evidence and thus unable to mount an effective defense through the approved lawyer.

Attempts to rectify this situation have taken various forms, from governments providing alternate, unclassified (redacted) documents to "gisting," or providing the central idea of, the arguments against the accused so they can provide defenses to their counsel. Though all of these are far better than providing no information at all, all are limited. This paper will argue for adding another tool to the existing range of options, government release of source/method modified information. This focuses on the idea of verisimilitude, or the appearance of truth. In brief, this technique would entail the government providing highly specific information, but information that has been created or modified so it appears to come from a different source from which it was actually derived. By creating a version of the information that resembles, but is not truly, classified information, it may be possible to reap many of the benefits of fuller disclosure without the associated costs.

Part I provides an overview of the Special Advocate system and the Classified Information Procedures Act (CIPA). These are the two institutionalized frameworks commonly used in Commonwealth countries and the United States.[6] This is essential for understanding where and how source/method modified information would be used. Further, exploring these systems highlights their current difficulties relaying information to defendants, a problem that may be partially curable with source/method modified information. Part II explains source/method modified information in more detail, examining current meth-

6. There are other systems that handle national security cases, for example military commissions. However, the Special Advocate system and CIPA represent two of the major frameworks in common law countries.

ods of redaction and showing the distinctions between the two. It also details the specific benefits to parties involved, including the public benefits to using such a policy. In doing so, it explores the concept of verisimilitude in the national security context. Part II then looks at the role of the judiciary in ensuring that source/method modified information is integrated into existing processes and not misused. Part III looks at the limits of source/method modified information and objections to its use, including the impact modified documents would have on the court and the possible public perception of such a policy. It invites weighing of these factors to determine the appropriate uses of source/method modified information.

I
Overview of the Existing Process

A. Special Advocate System in the U.K. and Canada

A number of western liberal democracies have created a system that has come to be called the "Special Advocate" system, wherein a government-appointed lawyer has access to the classified information and argues on behalf of the defendant.[7] The system was born out of immigration cases. Under the Canadian Immigration Act of 1976, immigration decisions based on classified information would have to go through government review, including an independent external review body that protected the immigrant's interests in closed proceedings involving sensitive information.[8] Though Canada's legislation has since changed,[9] cleared lawyers have remained part of the Canadian system and are now officially referred to as "Special Advocates."[10]

7. This includes Canada, the U.K., and New Zealand. The United Nations High Commissioner for Refugees has recommended Australia use a similar system in refugee cases. Office of the U.N. High Comm'r for Refugees, Inquiry into Australia's Immigration Detention Network: Supplementary Submission on Special Advocate Mechanism 1.3 (Dec. 16, 2011).

8. *See* Immigration Act, 1976, R.S.C. 1976–77, c. 52, s. 1 (Can.); Canadian Security Intelligence Service Act, R.S.C., 1985, c. C-23. More on the Canadian Security Intelligence Review Committee is available on the internet at http://www.sirc-csars.gc.ca/.

9. In late 2001, Canada enacted the Immigration and Refugee Protection Act, S.C. 2001, c.27, which eliminated the aforementioned review process. This was successfully challenged in court, leading to Bill C-3, which recreated review with Special Advocates. For more information see Maureen T. Duffy, *Security Detention in Practice: Constitutional Canaries and the Elusive Quest to Legitimize Security Detentions in Canada*, 40 Case W. Res. J. Int'l L. 531, 541 (2009). *See also* Charkaoui v. Canada, [2007] 1 S.C.R. 350 (Can.).

10. *Frequently Asked Questions: Bill C-3 and Special Advocates*, Dep't of Justice (Aug. 3, 2012), http://www.justice.gc.ca/eng/dept-min/sa-as/faq.html [hereinafter *Bill C-3 FAQs*] (Can.).

Special Advocates are intended to enable the use of classified information in proceedings while maintaining a fair hearing for the accused, who do not have access to this information.[11] This idea of using government-appointed lawyers spread both geographically and jurisdictionally. In *Chahal v. United Kingdom* the European Court of Human Rights looked approvingly on the use of Special Advocates as a balance between state security interests and preserving a fair hearing for the accused.[12] Accordingly, in the wake of this decision, the United Kingdom passed the Special Immigration Appeals Commission Act 1997, which adopted a Special Advocate system modeled on Canada's.[13] During the U.K.'s legislative debates regarding Special Advocates, the system was described as, "necessary to protect the public interest in not disclosing . . . sensitive material, while allowing independent scrutiny of that sensitive material."[14] Though this system began in exceptional immigration contexts, the use of Special Advocates has since expanded. In the U.K. for example, there are now a number of tribunals and courts with security concerns that use Special Advocates ranging from employment tribunals to control orders.[15]

Simply put, Special Advocates are lawyers who have been cleared to view classified information and represent the interests of the accused.[16] These individuals are not the Defendant's lawyers in the traditional sense, however. In the U.K. they have been referred to as "litigation friend[s],"[17] there to "ensure that the rights of the appellant

11. *Id.*

12. Chahal v. United Kingdom, App. No. 22414/93, Eur. Ct. H.R. (1996).

13. Special Immigration Appeals Commission Act, 1997, c. 68 (U.K.). *But see* David Jenkins, *There and Back Again: The Strange Journey of Special Advocates and Comparative Law Methodology*, 42 COLUM. HUM. RTS. L. REV. 279, 300 (2011) (arguing that the U.K.'s system was modeled on what they thought the Canadian system to be, but that the European Court of Human Rights actually misunderstood the Canadian system).

14. CONSTITUTIONAL AFFAIRS COMMITTEE, SEVENTH REPORT: THE OPERATION OF THE SPECIAL IMMIGRATION APPEALS COMMISSION (SIAC) AND THE USE OF SPECIAL ADVOCATES, 2004–05, H.C. 232-I, ¶ 48 (U.K.).

15. *Id.* at ¶ 50; ALEXANDER HORNE, HOME AFFAIRS SECTION, SPECIAL ADVOCATES AND CLOSED MATERIAL PROCEDURES, SN/HA/6285, at 4 (June 25, 2012) ("The use of Special Advocates expanded significantly"); Andrew Boon & Susan Nash, *Special Advocacy: Political Expediency and Legal Roles in Modern Judicial Systems*, 9 LEGAL ETHICS, 101, 104–05 (2006). Control orders are restrictions on a suspect's liberty to protect the public from terrorism. The restrictions are tailored to the suspect and include restrictions such as limiting the place of residence or work or limiting who they may contact. For more on control orders see Dominic McGoldrick, *Security Detention in Practice: Security Detention-United Kingdom Practice*, 40 CASE W. RES. J. INT'L L. 507 (2009).

16. *Bill C-3 FAQs*, *supra* note 10.

17. CONSTITUTIONAL AFFAIRS COMMITTEE, *supra* note 14.

are protected."[18] Special Advocates buttress the defendant's legal team by providing representation in closed proceedings involving classified information but do not participate in the open portions of the trial. Thus, the defendant's counsel still argues the open material and provides guidance to the defendant, but is replaced by the Special Advocate in closed hearings.[19] The advocate has two primary functions in these proceedings:

> First . . . to challenge government claims that certain information must remain confidential . . . . Second, [to] participate in the closed hearings by cross-examining government witnesses who testify, and by making submissions on the relevance, reliability and sufficiency of the government's evidence.[20]

By fulfilling this function the Special Advocate ensures that the adversarial nature of the trial is maintained even during closed proceedings. This removes the unfairness of having one side able to present evidence and witnesses unquestioned by the other. It also limits the government's ability to hold evidence it should disclose to the accused by allowing a party with access to challenge their claims.

Though Special Advocates have more access to complete information than the defendant's lawyers, their roles are also limited in important ways. Two major limitations are the advocate's access to the defendant and the scope of their arguments.

The advocate's access to the defendant is limited in a fundamental way. Once the advocate has viewed the closed material they "cannot take instructions (subject to narrow exceptions) from the persons they are representing or their ordinary legal representatives."[21] This has been described as "undoubtedly the most serious limitation on what Special Advocates can do."[22] Further, they cannot disclose closed materials to the Defendant.[23] Their meaningful contact with defendants is thus at more preliminary stages, before they view or argue the closed materials. Even the aforementioned narrow exceptions to the communications rules may be too circumscribed. Canadian law

---

18. *Id.*

19. *See generally* SECRETARY OF STATE FOR JUSTICE, JUSTICE AND SECURITY GREEN PAPER 52 (2011) (U.K.).

20. *Bill C-3 FAQs*, *supra* note 10.

21. CONSTITUTIONAL AFFAIRS COMMITTEE, *supra* note 14, at ¶ 52.

22. CONSTITUTIONAL AFFAIRS COMMITTEE, SEVENTH REPORT: THE OPERATION OF THE SPECIAL IMMIGRATION APPEALS COMMISSION (SIAC) AND THE USE OF SPECIAL ADVOCATES, 2004–05, H.C. 232-II, EV 55 ¶ 8 (U.K.).

23. *Canada: Parliament Should Amend Bill on Special Advocates*, HUMAN RIGHTS WATCH (Nov. 19, 2007), http://www.hrw.org/news/2007/11/18/canada-parliament-should-amend-bill-special-advocates.

does not guarantee that the Special Advocate will be able to meet with the defendant; instead, any such meeting requires judicial authorization.[24] U.K. law is incredibly similar, with the advocate needing authorization to speak to the defendant once they have seen the classified materials.[25] Notably, though authorization is theoretically possible, it is incredibly rare.[26] This means it is imperative the accused be able to communicate defenses to the advocate in very early stages of the proceedings. To do this, the accused would need to know something of the evidence against him or herself to communicate defenses, such as alibis, with the advocate before the closed proceedings commence.

The second major limitation is directly related to the first. The Special Advocate's scope is limited in that they only make arguments about the closed materials they are privy to; arguments based on open material are not within the purview of the Special Advocate and instead fall to the traditional defense counsel. Though the Special Advocate does have full access to the classified information, including confidential human sources and details revealing intelligence methods, this does not enable a full and well-rounded defense. Due to limited scope and communication/access issues, the defense will almost inevitably be fragmented and a defense strategy may be made exponentially more difficult to maintain.[27] That is, while the Special Advocate may be able to question sources or methods used, they may not know if the accused has a response to a government allegation at all and may not be able to pair their responses in closed hearings to the defendant's claims in open proceedings.[28] Conversely, the government can coordinate its responses across hearings.

In an effort to overcome these problems, courts have held that defendants must be told something of the charges against them.[29] Without this, the Special Advocate is likely to be ineffective and the

24. *Id.* ("[A]fter review of secret evidence the SA would require judicial authorization to communicate with any other person about the proceeding (s. 85.4(2)), which would include any discussion on the substantive nature of the evidence").

25. Boon & Nash, *supra* note 15, at 103–04.

26. *Id.* at 104 & n.25 (noting that Special Advocates emphasized "that in practice there was no contact"). However, communication is not cut off entirely. The accused may still write to the advocate though they will not have access to the information and the advocate is unlikely to be able to communicate back.

27. One can imagine, for example, defense counsel in an open proceeding arguing that this is a case of mistaken identity and an advocate arguing that the secret evidence indicates the defendant was acting under duress. While these may not be incompatible per se, it may be more effective to have a single, unified, defense strategy.

28. CONSTITUTIONAL AFFAIRS COMMITTEE, H.C. 232-II, *supra* note 22, at EV 55.

29. *See, e.g.*, Sec'y of State for the Home Dep't v. AF (No. 3), [2010] EWHC 42 (Admin.) (U.K.); A. v. United Kingdom, App. No. 3455/05, Eur. Ct. H.R. (2009).

proceeding can no longer be considered fair. This process, known as "gisting" is by no means clear however.[30] In *Chahal*, the court seemed to presume that it was possible to relay a summary of the evidence to the accused.[31] Though discussed by the court, there is nothing in the Special Immigration Appeals Commission Act, 1997 that explains the contours of this disclosure.[32] The question of relaying information to the accused was thus revisited in *A. v. United Kingdom*.[33] Among a number of defendants, two were alleged to have been financiers for Al Qaeda based on classified information. Evidence to this effect was not relayed to the defendants however, even in a redacted or gisted form.[34] The court attempted to balance the state interest in security against article 5.4[35] convention rights in having a fair trial.[36] Though the court did not set a bright line for what information was to be disclosed they did hold that there must be sufficient disclosure for a defendant to "effectively . . . challenge the allegations against them."[37] This standard was later adopted by the House of Lords for alleged violations of Article 6.1[38] of the European Convention on Human Rights,[39] though

30. ANGUS MCCULLOUGH ET AL., JUSTICE AND SECURITY GREEN PAPER: RESPONSE TO CONSULTATION FROM SPECIAL ADVOCATES, 17 at n.24, *available at* http://consultation.cabinetoffice.gov.uk/justiceandsecurity/wp-content/uploads/2012/09_Special%20Advocates.pdf. Gisting is simply providing a summary of the key facts. For an example of a rather comprehensive gist, unlike those cases previously identified, see CF v. Sec'y of State for the Home Dep't, [2013] EWHC 843 (U.K.).

31. Chahal v. United Kingdom, App. No. 22414/93, Eur. Ct. H.R. (1996).

32. *See generally* Special Immigration Appeals Commission Act, 1997, c. 68 (U.K.).

33. A. v. United Kingdom, App. No. 3455/05, Eur. Ct. H.R. (2009).

34. *Id.* at ¶¶ 223–24.

35. "Everyone who is deprived of his liberty by arrest or detention shall be entitled to take proceedings by which the lawfulness of his detention shall be decided speedily by a court and his release ordered if the detention is not lawful." Convention for the Protection of Human Rights and Fundamental Freedoms, Nov. 4, 1950, art. 5.4, 213 U.N.T.S. 221 [hereinafter European Convention on Human Rights].

36. A. v. United Kingdom, App. No. 3455/05, at ¶¶ 216–17. For more on article 5 of the European Convention on Human Rights see COUNCIL OF EUROPE, DIRECTORATE GENERAL OF HUMAN RIGHTS, THE RIGHT TO LIBERTY AND SECURITY OF THE PERSON: A GUIDE TO THE IMPLEMENTATION OF ARTICLE 5 OF THE EUROPEAN CONVENTION ON HUMAN RIGHTS (2002).

37. A. v. United Kingdom, App. No. 3455/05 at ¶ 224.

38. "In the determination of his civil rights and obligations or of any criminal charge against him, everyone is entitled to a fair and public hearing within a reasonable time by an independent and impartial tribunal established by law. Judgment shall be pronounced publicly but the press and public may be excluded from all or part of the trial in the interests of morals, public order or national security in a democratic society, where the interests of juveniles or the protection of the private life of the parties so require, or to the extent strictly necessary in the opinion of the court in special circumstances where publicity would prejudice the interests of justice." European Convention on Human Rights 6.1.

it is not entirely clear if the standard set forth parallels the previously understood gisting requirement.[40] Though there is a consensus that information should be relayed to the accused in some way, judges have left open the possibility there may be cases where relaying information is impossible but failing to do so is not inherently unfair.[41] Regardless of the circumstances, however, relaying information to the accused may take multiple forms including "redaction, anonymization, and gisting."[42]

B. CIPA in the United States

The United States does not use the Special Advocate framework. Instead, criminal cases involving classified information in the United States are governed by the Classified Information Procedures Act (CIPA).[43] CIPA governs the use of classified information in traditional court settings, from discovery until disposition.[44] Under CIPA either party may call for a pretrial conference pertaining to the use of classified information,[45] and the government can request that the court issue a "protective order" that restricts disclosure to the defendant.[46] The government may also ask the court to limit disclosure of classified information as early as discovery through an *ex parte* hearing.[47] When the court authorizes this the government is to "substitute a summary of the information for such classified documents, or to substitute a statement admitting relevant facts that the classified information would tend to prove."[48] In essence, the government must replace classified information with unclassified information.

---

39. *See* Home Sec'y v. AF, [2009] UKHL 28, (appeal taken from Eng.).
40. *See supra* note 30.
41. Sec'y of State for the Home Dep't v. MB, [2007] UKHL 46, [90] (appeal taken from Eng.) (leaving open the possibility that there will be cases where the judges "feel quite sure that in any event no possible challenge could conceivably have succeeded").
42. *Id.*
43. Classified Information Procedures Act (CIPA), 18 U.S.C. app. 3 §§ 1–16 (2012). There is some discussion of using this system in the U.S. immigration context as well. *See End Government Use of Secret Evidence Against Immigrants*, ACLU, http://www.aclu.org/end-government-use-secret-evidence-against-immigrants (last visited Sep. 4 2013). In the case of removal proceedings for lawful permanent aliens, the proceedings bear remarkable similarity to the Special Advocate system. For example, the court appoints a "special attorney" who reviews and argues the material in closed proceedings and is forbidden to disclose any of the information to the defendant. 8 U.S.C. § 1534(e)(3) (2011).
44. CIPA § 2.
45. *Id.*
46. *Id.* § 3.
47. *Id.* § 4.
48. *Id.*

CIPA also addresses the defendant's use of classified information, requiring that defendants reasonably expecting to disclose classified information notify the government and court.[49] The concept that the defendant would seek to utilize classified information against the government is a product of CIPA's legislative history. CIPA was originally created in 1980 to deal with situations of graymail, particularly in cases of information leaks or espionage.[50] Defendants in espionage cases were threatening to disclose highly classified information in trials, making it difficult for the government to litigate such cases.[51] However, CIPA is now used more broadly, including in cases related to terrorism.[52] When the government wishes to object to the use of classified information at trial, they may request a hearing.[53] Through these hearings the government has the ability to substitute classified documents for a summary of the information or a statement admitting relevant facts.[54] This is not absolute however, it is tailored by a provision that the substitute document must allow the accused "substantially the same ability" to make their defense.[55]

Through the text of the statute, CIPA is thus distinct from the Special Advocate system in a number of ways. First, there is no specially appointed lawyer. Second, there is no provision that expressly limits the lawyer's contact with the defendant. Third, underlying CIPA is the idea that in some situations it will be the defendant, not the government, seeking to introduce classified information.

Later jurisprudence complicates this picture. Pursuant to CIPA the Chief Justice of the United States Supreme Court created rules protecting classified information in courts.[56] One of these rules is that the government may obtain information on individuals acting for the defendant and, "bring such information to the attention of the court for the court's consideration in framing an appropriate protective order

49. *Id.* § 5.

50. LARRY M. EIG, CONG. RESEARCH SERV., CLASSIFIED INFORMATION PROCEDURES ACT (CIPA): AN OVERVIEW 1–3 (1989), *available at* http:// www.fas.org/sgp/crs/secrecy/89-172.pdf (last visited Sep. 5, 2013). "Graymail" refers to situations in which a defendant who had access to classified information would threaten to expose it at trial as part of their defense, forcing concessions from the government. *Id*.

51. *Id.*

52. *See, e.g.*, In re Terrorist Bombings of U.S. Embassies in E. Afr., 552 F.3d 93 (2d Cir. 2008).

53. CIPA § 6(a).

54. *Id.* § 6(c)(1)(A)–(B).

55. *Id.* § 6(c)(1).

56. *Id*. § 9(a).

pursuant to Section 3 of the Act."[57] This has had the effect of requiring that defense lawyers be cleared to have access to any classified information.[58] That is, the government may simply use § 3 to have a protective order issued, preventing un-cleared lawyers from being able to see the information.[59] This logic extends to the accused themselves as well. If the defendant cannot obtain a clearance, their lawyer would not be able to share classified information with them.[60] In situations where neither the accused nor their counsel were able to obtain clearances, courts have appointed cleared lawyers to represent the defendant in the closed proceedings.[61]

There are thus a number of similarities between the Special Advocate system and CIPA. Not only have both expanded in scope, but the two have the same goal, "to harmonize a defendant's right to obtain and present exculpatory material upon his trial and the government's right to protect classified material in the national interest."[62] In both CIPA and the Special Advocate system there are also methods for relaying information that would otherwise be protected. These include redaction, summarizing, and admitting facts the classified information "would tend to prove."[63] In the Special Advocate system there is a small, defined, pool of lawyers; under CIPA the defense counsel must be cleared, a *de facto* limitation, and in some cases the court even appoints lawyers.[64] In both, the lawyers may not be able to discuss the classified information with the accused.[65]

---

57. SECURITY PROCEDURES ESTABLISHED PURSUANT TO PUB. L. 96–456, 94 STAT. 2025, BY THE CHIEF JUSTICE OF THE UNITED STATES FOR THE PROTECTION OF CLASSIFIED INFORMATION, ¶ 5.

58. *See* United States v. Bin Laden, 58 F. Supp. 2d 113 (S.D.N.Y. 1999) (holding that defense counsel was required to obtain a security clearance); David I. Greenberger, Note, *An Overview of the Ethical Implications of the Classified Information Procedures Act*, 12 GEO. J. LEGAL ETHICS 151, 166 (1998) ("Defense counsel have often argued that CIPA is unfair because it requires them to undergo security clearances.").

59. In *United States v. Jolliff*, 548 F. Supp. 232 (D. Md. 1981) the Defendant unsuccessfully argued that this requirement violated his Sixth Amendment right to counsel.

60. *See* EDWARD C. LIU & TODD GARVEY, CONG. RESEARCH SERV., R41742, PROTECTING CLASSIFIED INFORMATION AND THE RIGHTS OF CRIMINAL DEFENDANTS: THE CLASSIFIED INFORMATION PROCEDURES ACT R41742, 3 (1989), *available at* http://www.fas.org/sgp/crs/secrecy/R4172.pdf (last visited Sep. 5, 2013) ("Courts may issue protective orders prohibiting cleared counsel from sharing any classified information with the defendant").

61. *Id*. In these situations CIPA is incredibly similar to the Special Advocate system.

62. United States v. Wilson, 571 F. Supp. 1422, 1426 (S.D.N.Y. 1983).

63. Classified Information Procedures Act (CIPA), 18 U.S.C. app. 3 § 4(d) (2012).

64. EIG, *supra* note 50.

65. CIPA §§ 1–16; MCCULLOUGH, ET. AL., *supra* note 30; Reid *infra* note 81.

C. Problems with the Current Systems and Inherent Tensions

Though both these systems attempt to strike a balance between competing interests, critics have claimed that the systems are fundamentally flawed in a number of ways. Critics have gone as far as to call the U.K.'s system "Kafkaesque,"[66] Canada's "unconstitutional and unfair,"[67] and CIPA a violation of a host of rights.[68]

There are a number of system specific criticisms. One criticism of the Special Advocate system is that because the advocates are appointed by the court they may be perceived as serving government interests rather than the interests they are intended to represent.[69] CIPA has been criticized for functioning outside of its intended purpose. A number of scholars have distinguished the graymail cases for which CIPA was designed from modern terror-related cases.[70] In the former, the accused had access to the classified information as they had leaked it or were engaged in espionage. In modern terrorism-related cases, the defendant does not have the same background information on the classified information in question. In fact, they may have no idea what is contained in the government's classified documents. Whereas a spy knows the information he stole and may threaten to reveal it, an alleged terrorist likely does not have access to any classified information and, as such, cannot possibly reveal it.[71]

---

66. *Canada: Parliament Should Amend Bill on Special Advocates*, HUMAN RIGHTS WATCH (Nov. 18, 2007), http://www.hrw.org/print/news/2007/11/18/canada-parliament-should-amend-bill-special-advocates.

67. Kirk Makin, *'Special Advocate' Ruling a Partial Victory for Ottawa in Terror Case*, GLOBE & MAIL (Sep. 6, 2012, 12:52 PM), http://www.theglobeandmail.com/news/politics/special-advocate-ruling-a-partial-victory-for-ottawa-in-terror-case/article4102481/.

68. Laura Rovner & Jeanne Theoharis, *Preferring Order to Justice*, 61 AM. U. L. REV. 1331, 1386–89 (2012).

69. *See* Cristin Schmitz, *Independence Controversy Swirls Around New Special Advocates*, LAWYERS WKLY. (March 28, 2008), *available at*, http://www.lawyersweekly.ca/index.php?section=article&articleid=642.

70. *See* Committee on Communications and Media Law of the Association of the Bar of the City of New York, *The Press and the Public's First Amendment Right of Access to Terrorism on Trial*, http://www.nycbar.org/pdf/report/Medial%20Law%20Comm%20Report%20doc.pdf (lasted viewed on Sept. 8, 2013).

71. Note that this argument may be faulty. A falsely accused spy may not have the secrets the government claims they possess and thus may not be able to graymail the government. Graymail works when the accused really does have access to classified information they can credibly threaten to release, knowing it will harm the national interest. This may be more parallel to one who has engaged in terror related activity. While it is correct this does not provide them with graymail per se, they should still know the substance of the accusation against them.

A deeper problem, one common to both systems, was raised by Lord Bingham in *Regina v. H and C*.[72] A Special Advocate "cannot take full instructions from his client, nor report to his client . . . is not responsible to his client and [his] relationship with the client lacks the quality of confidence inherent in any ordinary lawyer-client relationship"[73] and is, as a result, "acting in a way hitherto unknown to the legal profession."[74] As aforementioned, communication barriers create one of the largest problems with the Special Advocate system. Special Advocates have no means of coordinating defenses, planning responses to allegations based on closed material, or having any sort of iterative process to interact with the accused. All of this makes the process extremely unfair.[75] This criticism is not isolated. In response to a government paper on closed proceedings and Special Advocates, all but twelve of the U.K.'s Special Advocates responded by writing that the proceedings were "inherently unfair."[76] This was in part because Special Advocates are unable to take instructions and thus have great difficulty responding effectively to government charges.[77] Indeed, in enumerating problems with the U.K.'s current process the first item on their list was the prohibition on direct communication with the accused once the Special Advocate has seen the closed materials.[78] The US system has fared no better on this issue. Critics claim CIPA "threatens to erode the adversarial process that is at the heart of and necessary for just criminal prosecutions."[79] Among other things, this is because CIPA deprives defendants of their Sixth Amendment rights by preventing communication regarding classified materials with the defendant.[80] As with the Special Advocate system, the defen-

72. *See* Regina v. H & C, [2004] UKHL 3.

73. *Id*. at ¶ 22.

74. *Id.*

75. *See* Henry J. Friendly, *"Some Kind of Hearing,"* 123 U. PA. L. REV. 1267 (1975) (discussing the factors that make for an adversarial hearing, such as the right to know opposing evidence, the grounds for a proposed action against oneself, and the right to cross examine witnesses).

76. MCCULLOUGH ET AL., *supra* note 30. The other twelve did not object to any of the findings of the consultation. *See* Tim Otty*, The Slow Creep of Complacency*, 3 EUR. HUM. RTS. L. REV. 267, n.vi (2012).

77. MCCULLOUGH ET AL., *supra* note 30, at 5.

78. *Id.* at 7.

79. Rovner, *supra* note 68, at 1389.

80. Joshua L. Dratel, *Ethical Issues in Defending a Terrorism Case: How Secrecy and Security Impair the Defense of a Terrorism Case*, 2 CARDOZO PUB. L. POL'Y & ETHICS J. 81, 100 (2003). Dratel argues that CIPA violates a number of other rights and also highlights *United States v. Moussaoui*, No. Crim. 01-455-A, 2002 WL 1311718 (E.D. Va. Apr. 17, 2002) wherein a 9/11 pro se defendant was thus unable to access large amounts of information.

dant's inability to meaningfully engage with classified materials is seen as the heart of the problem.[81]

The problem with simply allowing communication is clear, however. Governments may fear that discussion of information would compromise ongoing operations or betray intelligence assets.[82] Lord Carlile of Berriew explained it this way: "The rationale . . . is that one may be dealing with terrorists who are so skilled and subtle that almost whatever you say to them will enter their understanding in a very lateral way, and they will be able to deduce, for example, that certain places are being watched, or certain communications are being listened to."[83] Governments may also fear that classified information will become widespread and will therefore more likely be released to the public. CIPA for example, was created to combat leaks.[84] Regardless of whether one focuses on the accused or the public, the danger of information being revealed is the same: by one path or another, the information may find its way to a hostile element and intelligence assets or operations would be compromised.[85] Further, it may be more difficult to recruit intelligence sources as they would feel less secure and costly technical intelligence platforms could be rendered useless with countermeasures.[86] To apply this logic to the court system is not a sign of distrust in the court system or the accused specifically; rather, this is a foundational tenet of classified information. Even within the government, individuals must undergo rigorous clearance processes and are given access to narrow spectrums of information based on "need to know."[87]

Another way of understanding this concern is that openness in judicial proceedings opens three paths for sensitive information to get out. The first is that mentioned by Lord Carlile of Berriew, through

---

81. Melanie Reid, *Secrets Behind Secrets: Disclosure of Classified Information Before and During Trial and Why CIPA Should Be Revamped*, 35 SETON HALL LEGIS. J. 272, 292 (2011).

82. Boon, *supra* note 15, at 103–04 (explaining the risk of "contamination").

83. HOME AFFAIRS COMM., MINUTES OF EVIDENCE: EXAMINATION OF WITNESS, ¶ 84 (11 March 2003) (U.K.).

84. *See Graymail Legislation: Hearing Before the Subcomm. on Legislation of the H. Permanent Select Comm. on Intelligence*, 95th Cong. (1979);? *The Use of Classified Information in Litigation: Hearing Before the Subcomm. on Secrecy and Disclosure of the S. Select Comm. on Intelligence*, 95th Cong. (1978).

85. Reid, *supra* note 81, at 278 ("disclosure of classified information to unauthorized personnel could result in the exposure and loss of valuable sources and methods which are vital to national security.").

86. *The Use of Classified Information in Litigation: Hearing Before the Subcomm. on Secrecy and Disclosure of the S. Select Comm. on Intelligence*, 95th Cong. 12–13 (1978) (statement of Adm. Stansfield Turner, Director of Central Intelligence).

87. Exec. Order No. 13,526, 3 C.F.R. 298, 314 (2009).

the defendant.[88] Even from a jail cell it may be possible for the accused to get information to his or her compatriots. The second is through the court system itself—unless there are protective measures in place, the nature of proceedings may compromise the secret. A former CIA Director offered a hypothetical wherein a spy attempts to transmit a list of CIA assets to a foreign government but is captured on the way. If this list of assets were introduced as evidence in a typical trial, the spy would have succeeded; all the foreign government would have to do is obtain an open court record.[89] The third is through leaks, such as information being released to the press. The more people who have access to information, the more likely it is to be leaked.

The central problem is thus that there is a seemingly irreconcilable tension between the interests of a government in maintaining its secrets and the interest of the accused in having a fair trial wherein they can prepare an adequate defense. CIPA and the Special Advocate system both attempt to strike a balance between these interests, providing judicial proceedings in place of dismissal or non-judicial government action but limiting the use of sensitive information in recognition of security concerns. While critics accept that there is a tension between these interests, their arguments tend to be that the current models do not strike the proper balance between these goals, leaning too far in favor of one party or the other.

II
SOURCE/METHOD MODIFIED INFORMATION

A. Overview of the Proposed System

The theoretically optimal solution in both these systems is one in which there is a perfectly fair procedure for the accused but no additional risk of sensitive information being compromised. This is likely impossible, but there may be ways to get closer to this outcome. This is because the information that the sides are interested in learning and protecting does not fully overlap. That is, the government has an interest in protecting pieces of information that may be embedded in, but are not necessarily the substance of, what the defendant and their counsel wish to discuss or use at trial.

This is due to the distinction between sources, methods, and substance.[90] When the government explains its interest in protecting clas-

88. *See* HOME AFFAIRS COMM., *supra* note 83.

89. *The Use of Classified Information in Litigation*, *supra* note 86, at 12.

90. *See generally* DEP'T OF DEF., DIR. 5200.1-H, HANDBOOK FOR WRITING SECURITY CLASSIFICATION GUIDANCE (1999) [hereinafter DOD DIR. 5200.1-H]. *But see*

sified information it is often focusing on intelligence sources or methods and not as often on the substance of what they have learned. The degree to which substance is important is often the degree to which it betrays a source or a method.[91] For example, a list of intelligence agents in a country may be sensitive because it contains information on sources.[92] A record of a phone call may be sensitive because it reveals that the government has tapped the phone. There is however, distinct substance. That person X went to location Y may have been derived from any number of possible sources or methods, from geolocation[93] to a spy. Accordingly, the substance of this information is likely not to be sensitive in and of itself.[94] This is precisely the type of information that may be essential for the accused to have a fair hearing, however. While a defense may be made from the fact that a spy or geolocation was used, the core of a defense will likely revolve around the alleged actions of the defendant, which will be contained within the substance of the government's classified information. Communicating the alleged actions that constitute the elements of the offense thus enables a more vigorous defense.

The question is then whether there is a way to split substantive information from source/method information. If this can be done, the government could relay the one while protecting the other. If possible, this could be used in a number of ways to combat existing problems in either the Special Advocate or CIPA system. First, it may simply allow for more information to be presented to the accused. Additionally, it may allow for further procedural advancements for the accused. For example, if it becomes much less likely that the source or method will be revealed in conversation, it may be possible to allow advocates or cleared lawyers to discuss the substance of the allegations with the

---

Michael Warner, *Wanted: A Definition of "Intelligence,"* CENTRAL INTELLIGENCE AGENCY (June 27, 2008, 7:12 AM), https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol46no3/article02.html (concluding that there is not clear guidance or definitions on what constitutes "intelligence" or "sources and methods"). That the bounds of "intelligence" or "sources and methods" are murky does not necessarily mean they are indistinguishable, however.

91. *See, e.g.*, DoD DIR. 5200.1-H, *supra* note 90, at C6.1.3–6.1.4.

92. *Id.* at C6.1.14.4.

93. Geolocation is determining the real world location of an object based on its connection to a digital network. *See* Geolocation, WEBSTER'S ONLINE DICTIONARY, http://www.websters-online-dictionary.org/definitions/Geolocation (last visited Nov. 9, 2013). For example, determining the location of computers based on internet protocol addresses.

94. DoD DIR. 5200.1-H at C6.1.14.4; *see also* DEP'T OF DEF., MANUAL 5200.01, INFORMATION SECURITY PROGRAM: OVERVIEW, CLASSIFICATION, AND DECLASSIFICATION (2012) [hereinafter DoD MANUAL 5200.01].

accused as the government would not fear source/method information being released.

Currently, the bounds of what classified information can be transmitted to the accused seem to be drawn by what can be redacted or anonymized.[95] As such, I propose adding to the range of ways the government communicates information to the accused. In addition to existing options, the government would be allowed to issue source or method modified information, documents that retain the core accusations but rewrite sources and/or methods. This would serve both government interests by protecting valuable national security interests (the sources and methods) but also create another avenue for information to be relayed to the accused. As with redacted information, this source/method modified information would be available to the defendant and would become part of whatever public records contain the otherwise unclassified evidence and documents. This would serve to augment rather than replace existing means of transmitting sensitive information.

Source/method modified information protects sensitive information by replacing it with something else. In making these changes however, the government would retain the core substance of the information, material of value to the accused. This type of modification could take a number of different forms, each serving to protect a distinct government interest. In some situations the government will wish to protect a source of information, in others the means they used to gather it. There will likely be some in which the government seeks to protect both. Though the specifics of each case are likely to vary tremendously, there are a number of common themes that are likely to repeat themselves. These are modifications of source, method, or both source and method.

B. Source/Method Modified Information Contrasted with Current Forms of Redaction

Current methods of redaction or gisting work in a very different fashion. Typically redaction involves simply covering over or erasing classified portions of information.[96] This is not the only form of gov-

95. *See* Classified Information Procedures Act (CIPA), 18 U.S.C. app. 3 §§ 1–16, § 6(c) (2012).

96. *See, e.g.*, *Heavily-Redacted Documents Relating to the "Waterboarding" of Prisoners in CIA Custody*, ACLU (May 27, 2008), http://www.aclu.org/torturefoia/released/052708/ (providing links to a number of documents redacted by blacking out text).

ernment redaction however. In *United States v. North*[97] for example, the court took a different approach. *North* arose in the aftermath of Iran-Contra when an independent counsel was tasked with investigating and prosecuting government officials who were involved.[98] This led to the indictment and trial of Oliver North, a former official in the National Security Council, on several charges.[99] North sought to introduce classified information at trial, claiming that the Iran-Contra affair was ordered by higher-level officials.[100] As these documents implicated the locations of intelligence assets and activities, there was a CIPA § 6 proceeding to determine what should be done. The court decided that most of the information could be used at trial, but with several key restrictions. First, the names of intelligence officers were redacted and replaced with generic terms such as "CIA official."[101] Second, some geographic terms from classified documents were replaced with more generic ones such as "city" or "a European country."[102] Third, references to CIA facilities were replaced with benign and generic terms like "village" or "airport."[103] Additionally, information on intelligence methods remained classified and descriptions of such were replaced with phrases such as "reliable intelligence."[104]

Though *North* differs from simply erasing or covering over portions of the text, the overall effect is the same—the words or phrases that the government needs to protect are not relayed to the accused while the rest is. Redacted documents thus either replace or remove sensitive material altogether, presenting the remainder to the accused.[105] Source/method modified information would allow a more

97. *See* United States v. North, No. 88-0080-02, 1988 WL 148481 (D.D.C. Dec. 12, 1988) (order following CIPA § 6 *in camera* hearings).

98. United States v. North, 910 F.2d 843, 851 (D.C. Cir. 1990).

99. *Id.*

100. Anthony Lewis, *Abroad at Home; United States v. North*, N.Y. TIMES, Feb. 16, 1989, at A35.

101. 1988 WL 148481, at *2. (Applying only to those working in secret. If such persons testified, they could be given an identifier and the jury could be informed of that identifier in conjunction with the testimony.).

102. *Id.*

103. *Id.*

104. *Id.*; another take on North is provided in Jonathan M. Lamb, Comment, *The Muted Rise of the Silent Witness Rule in National Security Litigation: The Eastern District of Virginia's Answer to the Fight Over Classified Information at Trial*, 36 PEPP. L. REV. 213, 253–56 (2008).

105. *See Heavily-Redacted Documents*, *supra* note 96. *See also* NATIONAL SECURITY AGENCY, REDACTING WITH CONFIDENCE: HOW TO SAFELY PUBLISH SANITIZED REPORTS CONVERTED FROM WORD 2007 TO PDF (Mar. 18, 2008), *available at* http://www.nsa.gov/ia/_files/support/I733-028R-2008.pdf [hereinafter NSA REDACTION GUIDELINES] (providing an example of how one form of document is redacted by a member of the intelligence community).

thorough restructuring of the classified information, essentially relaying the same substance from a perspective sufficiently unique to disguise any sources or methods. Unlike redaction, the words relayed could be different from, and may be more than, what would be contained in a redacted document. Following are some examples of how and why such source/method modified information may be used:

Example 1: There has been an attempted VBIED.[106] A human source inside a terrorist organization identifies those responsible for the attempted attack. The government would like to charge those responsible for purchasing the explosives but does not want to do so at the risk of exposing its source. The government could use source/method modified information by creating documentation that routine monitoring of explosive precursors led to the discovery of the perpetrator. This allows for the government to provide very specific detail to the accused (when, how much, etc.) but does not compromise the source of the information.

Example 2: The government obtains access to a communication system a terror network believes impenetrable. While mining data the government obtains information about a specific terror cell they wish to use at trial. The government could introduce source/method modified information claiming that call chaining or human sources revealed the existence and structure of the cell. Further, they could replicate many of the details they know from their access to the network. Presenting the accused with "redacted" human source and call-chain information would give the accused a basis for defending themselves and communicating with counsel but would not leave the government with the accompanying fear that their access to the network would be detected and compromised.

Example 3: A government source in a hostile network has specific information the government wishes to use at trial. Instead of revealing the source, the government fakes a raid in which the source narrowly escapes, leaving behind the valuable information. Faked pocket litter and the like can be presented to the accused, providing specific details without fear the accused will believe the source was willfully cooperating with the government.

These also represent some of the different forms of modification. The first and second modify both the source and the method, the third modifies only the method.[107] One can also imagine the government

106. Vehicle Born Improvised Explosive Device.

107. One can argue that the second modifies only the source. Assuming this is a technical collection platform, it depends if such platforms are considered sources or

modifying only the source and keeping the method the same (e.g. claiming they had access to one person's phone when in fact they had access to another). These forms of modification may not always be beneficial but each of them adds to the number of possible ways in which otherwise classified information could be used in more traditional court proceedings.

Source/method modified information may thus be seen as both a form of redaction and distinct from redaction. It is similar to redaction in that its goals, and even techniques, are similar. Both seek to safeguard some information while relaying the rest. Further, cases like *North* suggest the courts accept substitution of terms.[108] At its most minimal, source/method modified information can be seen as an extension of this concept. Rather than replacing city X with a generic term, the government would be allowed to replace it with city Y. Source/method modified information departs from redaction however, in that it does not require that the information relayed to the accused be the verbatim remainder of the classified information. In that sense it can be seen as categorically distinct from redaction. Before examining the benefits of such a system in more depth, it is valuable to examine existing processes that seem conceptually similar to source/method modified information.

C. Derivation from Existing Judicial and Legislative Principles

The idea of presenting a half truth in court is not entirely new. Though this proposal may appear radical, it is actually derived from existing judicial procedures from a range of fields. Three areas in which truth is already obfuscated are cases involving personal identifying information; a number of criminal proceedings, for example, those involving undercover officers; and economic antidumping administrative proceedings.

The U.S. government had a source inside a dangerous gang, the Sinaloa Cartel, arguably the "largest and most powerful drug trafficking organization in the Western Hemisphere."[109] Needless to say, the cartel is a violent one.[110] The informant was present for a weapons deal and the delivery of ten pounds of methamphetamine, after which

---

methods. This is largely a semantic issue that has no bearing on the argument being made in this note, however.

108. *See* 1988 WL 148481.

109. *Sinaloa Cartel*, INSIGHT CRIME, http://www.insightcrime.org/groups-mexico/sinaloa-cartel (last visited March 30, 2013); Patrick Radden Keefe, *The Snow Kings of Mexico*, N.Y. TIMES MAG., June 17, 2012, at 37.

110. *See* INSIGHT CRIME *supra* note 109; Tracy Wilkinson, *Mexico Under Siege; Cartels Push Drug Violence to New Depths*, L.A. TIMES, May 28, 2012, at A1.

he identified one of the individuals involved to law enforcement.[111] Concerned for his safety if his identity was revealed to the cartel, the informant testified against the suspect while wearing a wig and fake mustache.[112]

Certainly there is a Sixth Amendment right to confront one's accuser.[113] Nonetheless, this right may be tempered in various ways.[114] When that individual is an undercover officer, or informant, as in the case above, the courtroom may be closed, they are often permitted to testify in disguise, and may not be required to identify him or herself by name.[115] Closing the courtroom and allowing undercover officers to testify with badge numbers are similar to redaction. In those instances the full accounting, there the name or physical appearance of the officer, is restricted for the safety of those individuals.[116] The use of disguise however, is more akin to source/method modified information. There, it is not simply that their true identity is protected but that the protection is in the form of their appearing different than they actually are.

Cases involving minors or personal identifying information are also commonly redacted.[117] In family court all the party's names may

111. United States v. De Jesus-Casteneda, 705 F.3d 1117 (9th Cir. 2013).

112. *Id.* at 3.

113. Bruton v. United States, 391 U.S. 123 (1968).

114. The government may not have to disclose the identity of an informant for example. The Court has held that there is not a bright line rule in this regard. *See* Roviaro v. United States, 353 U.S. 53, 62 (1957) ("The problem is one that calls for balancing the public interest in protecting the flow of information against the individual's right to prepare his defense. Whether a proper balance renders nondisclosure erroneous must depend on the particular circumstances of each case, taking into consideration the crime charged, the possible defenses, the possible significance of the informer's testimony, and other relevant factors").

115. Scher v. United States, 305 U.S. 251, 254 (1938) ("public policy forbids disclosure of an informer's identity unless essential to the defense, as, for example, where this turns upon an officer's good faith."); Ayala v. Speckard, 131 F.3d 62 (2d Cir. 1997) (allowing courtroom closures when undercover officers testified); People v. Mercado, 123 Misc. 2d 775 (N.Y. Crim. Ct. 1984) (holding that undercover officers may identify themselves by badge number instead of name).

116. The state's interest is made clear by the quote from the undercover officer in *Ayala*: "[w]hen asked what could happen if her identity was revealed to the public, she answered, 'Okay my cover could be blown and I could get killed.'" Ayala v. Speckard, 131 F.3d at 65. *See also* Benjamin Weiser, *Testifying Anonymously in Drug Case, Undercover Officer Describes the Fear of His Work*, N.Y. TIMES, April 23, 2003, at B3.

117. FED. R. CIV. P. 5.2 ("Unless the court orders otherwise, in an electronic or paper filing with the court that contains an individual's social-security number, taxpayer-identification number, or birth date, the name of an individual known to be a minor, or a financial-account number, a party or nonparty making the filing may include only: (1) the last four digits of the social-security number and taxpayer-identifi-

sometimes be redacted by the court.[118] In both the federal and state systems Social Security numbers and bank account information are often redacted as well, along with other information that may be used for identity theft.[119] As with the criminal proceedings, the ability to redact is not absolute. In Massachusetts, for example, redaction is not applicable where the information is necessary to "establish the identity of any person before the court."[120] These policies become more like source/method modified information when redaction becomes replacement. Arguably, this occurs with identifying minors not by their initials, but by characters not in their name. For example, courts using "X" or "John Doe" when they know the individual's name.[121]

There are also administrative processes that allow for incomplete or intentionally inaccurate information to be used. Antidumping regulations are one example of this. When a company submits information to the Department of Commerce as part of an antidumping proceeding, they often are required to submit proprietary information. To deal with this scenario, the Department of Commerce allows for companies to submit information for both an official and a public record.[122] However, the information for the public record may be modified to protect proprietary information. In these situations companies are allowed to substitute accurate proprietary information with a summary, including modified numbers, for public documents. For numeric values, this is explicitly allowed in two different ways, either by modifying the actual numbers within a specific range or "indexing," which involves creating a different number set that is scaled to the actual number.[123] For example, if two actual numbers in a set are 3,400 and 1,700 the indexed numbers could be 100 and 50.

Each of these examples contains redaction, which is accepted in our system, but hints at something more. Redacting personal informa-

---

cation number; (2) the year of the individual's birth; (3) the minor's initials; and (4) the last four digits of the financial-account number.").

118. *See, e.g.*, Dep't of Servs. for Children, Youth & Their Families v. C.S. (*In re* J.H.), 2007 Del. Fam. Ct. LEXIS 47 (Oct. 11, 2007).

119. *See, e.g.*, Mass. Supreme Jud. Ct., Interim Guidelines for the Protection of Personal Identifying Data in Publicly Accessible Court Documents (Sept. 1, 2009), http://www.mass.gov/courts/sjc/docs/interim-pid-guidelines.pdf; JUD. COUNCIL OF CAL., CA CT. RULE 1.20(b), (2008), http://www.courts.ca.gov/documents/title_1.pdf.

120. MASS. SUPREME JUD. CT., *supra* note 119.

121. *See* Arnold v. Bd. of Educ., 880 F.2d 305 (11th Cir. 1989) (using "John Doe" and "Jane Doe" to identify minors in the suit when it is evident their names were known).

122. DEP'T OF COMMERCE, *Access to Information*, *in* IMPORT ADMINISTRATION ANTIDUMPING MANUAL (2009).

123. *Id.* at 10.

tion or the name of a minor is accepted in both the federal and state systems. It seems to be well-accepted that the safety of undercover officers and informants must be protected in some way. It is understood that proprietary information cannot simply be released to the public or competitors. The link to source/method modified information arises when, instead of simply limiting, an alternate narrative is used by the court. For example, a child may be referred to as "X" though presumably their name does not begin with or contain the letter. John and Jane Doe are, likewise, not reflections of a true name. While this can also be seen as complete redaction, with X or John acting only as a place filler, one can imagine an innocuous name being used, a falsehood, to replace the real name.[124] The methods for protecting undercover officers are similar. While some have obvious parallels to redaction, such as using badge numbers or alternate forms of identification in place of a name, disguises are more similar to source modified information. There, the source of the accusation is made to look like something or someone it truly is not. The case of proprietary information is obvious: the summarized numbers may explicitly be different than the true ones.

Source/method modified information can thus be seen as an extension of existing judicial practices. Redaction is utilized throughout a range of proceedings. At points, however, the processes utilized seem to allow for more fundamental changes to information. Though none of these practices go as far as this paper's proposal for the national security context, they nonetheless indicate a level of judicial acceptance with modification of information. In the aforementioned circumstances, modification of truth in official documents is not used lightly. Nonetheless, it can be used, particularly when there are countervailing interests to full disclosure such as identity theft, business secrets, or the safety of law enforcement officials and their sources. This would be particularly pertinent if further research revealed that currently accepted levels of redaction or presenting half-truths scaled in relation to the gravity of the revelation. It is one thing if forms of redaction are narrowly tailored to meet their circumstances. However, if wigs and disguises are acceptable for undercover officers but not for hiding the identity of minors merely because the risk to life and limb is greater in most cases involving the former, this proposal may be appropriate given the extraordinary costs of classified information being released.[125]

124. If the judge decided to use "Bob Smith" or a random name generator instead of "John Doe," presumably there would be no basis for objection.

125. *See supra* notes 79–83 and accompanying text.

D. Benefits to Parties

1. Benefits to the Defendant

This adds another option for the government to relay information to the accused and can either supplement or replace other tools, providing more information for the accused to mount a defense. Source/method modified information fills a specific role that other forms of relaying information may not be able to fill. Redaction, for example, may not be possible if a document, however redacted, would still reveal the method by which the information was obtained.[126] A redacted phone transcript may still reveal that the government had access to a phone system. Summarizing the information would seem to accomplish the same goals as source/method modified information. However, there may be situations where the government feels that it cannot summarize the information for some reason. One reason would be if information would seem discordant without including some explanation of source or method to account for gaps or specific pieces of information.

Information tells a story; it forms a narrative elucidated through court proceedings.[127] Classified information is so difficult because there are parts of the narrative that cannot be told, pieces the government does not want in the public domain. There will be instances where the story can be abridged, a metaphorical chapter skipped while the narrative retains continuity. These can be seen as representing cases wherein redaction may be used. Other times this will not be possible—these are the examples discussed above that may be aided by source/method modified information. There, the sensitive information is so central to the narrative or contains a fact so pivotal that the story is little more than a bundle of disjointed words without that information. Currently those words must be discarded. That is, the government either cannot use the information at all or the defendant cannot have any access to it.

---

126. The ACLU documents previously cited are an example of how a redacted document may still have no value to a defendant, assuming it was released at all. The document labeled "Cable 333" for example, is almost entirely blacked out—entire pages are missing and others have single phrases with no meaningful context. *Heavily-Redacted Documents*, *supra* note 96. Additionally, the redaction process may leave classified information in metadata. As a result, redacting a classified document may require an extensive process. *See, e.g.*, NSA REDACTION GUIDELINES, *supra* note 105 (providing 14 pages of guidance on simply converting redacted Word documents to PDFs).

127. This is recognized, albeit indirectly, by the Court when they consider the prejudicial impact that pieces of evidence may have. *See* Old Chief v. United States, 519 U.S. 172, 180 (1997).

With stories, one can create an alternate framework for the words, repurposing them to tell a safer story. For example, if a parent wishes to explain a story involving birth to a child they may substitute science for a story involving a stork. By using the stork they avoid the material they would rather not cover at the time but allow the story to have both detail and continuity. They could, for example, discuss how the parents felt about the stork delivering the baby. In doing so, they convey the core information in question—the appearance of a child or the parents' feelings about it—without discussing the information they deem unacceptable. If the core information they needed to relay was the appearance of a baby in the story, the truth or falsity of the stork is of no consequence to the continuity of the story. Clearly defendants and their counsel are not children, but their access to information is nonetheless limited. There exist narratives that can be retold to convey critical information without relaying certain facts. Though this may bring complications, the alternative may be simply not relaying the story at all. In so much as intelligence information parallels narrative structures, it seems safe to assume this would likely be true in the context of classified information.

This leads to two distinct benefits for the accused. First, it may be possible to transmit more information to the accused. This carries with it the obvious benefits of being able to mount a more effective defense. The second benefit is that this may open channels for increased communication between the accused and their counsel or Special Advocate. Because there is a "cover story" of sorts, the government may not fear that information getting out would harm sources or methods as the counsel or Special Advocate could treat the source/method modified information as the entire truth in discussions and there would be no fear of inadvertent disclosure.

Though this form of information would not be of use to the defendant if they were challenging the veracity of the source, it does allow for a number of defenses that would be unavailable if there were no information or the information given the defendant was excessively general. Mistaken identity, for example, may be easier to make out if the accused has more specific information regarding the allegations. For such a defense, the source or method is irrelevant and the pertinent question is the timing and substance of the allegations. That is, if someone can provide an alibi that they were in a different location when they supposedly broke a law they can mount a defense, regardless of the source of the information. To critique the veracity of the actual source, the defense would have to use the tools already availa-

ble to them in their jurisdiction, either a Special Advocate or their cleared lawyer in closed proceedings.

Though the defendant is unable to directly critique sources, source/method modified information may still allow for more tailored questioning of source veracity. This is because as the narrative becomes richer the defendant may be able to object to specific portions of the allegations. This may in turn cause the Special Advocate or cleared counsel to examine the credibility of the actual sources more closely than they otherwise would have. For example, with a gist or heavily redacted summary the defendant may be in a situation where they are admitting or denying very general claims. If instead they had more detail, they may admit to one portion while denying others. This in turn could cause the cleared lawyer to focus on the veracity of the specific sources making claims the defendant is denying. Such focus may have broader implications relating to the credibility or admissibility of other witnesses or evidence, greatly aiding the defendant's case.[128]

It is evident that at least in some cases the government may be able to piece together an alternate source/method description that would allow for more information to be presented to the defendant, but this is not the only reason the flow of information may increase. Another reason the government may supply more information is that it may fear even summarized information would allow hostile counterintelligence elements to derive sources and/or methods. By allowing the government to present a modified source or method they may be able to alleviate these concerns by intentionally leading counterintelligence down rabbit holes.[129] For example, intentionally omitting a fact that would have been in electronic metadata may lead a hostile

128. For example, if the defendant strenuously objected to a single claim and the special advocate or cleared counsel could undermine the credibility of that source, they may find the same source or method served as the basis for other parts of the government's argument. Impugning the credibility of a human source or creating doubt that a phone was in the defendant's possession may thus aid the defendant in relation to other claims made on evidence from the same source. Notably, such information would likely be of benefit to the government as well, as source credibility undoubtedly plays a large role in accurate intelligence assessments.

129. *See* Section II(D)(2), *infra*. If there is any concern that this would prove an inverse, i.e. 'the government said the information came from x so really it must have come from y' this is alleviated in two ways. First, that logic is only applicable when the source set is tightly constrained (X or Y. Not X, ergo Y). If the range of sources is sufficiently large (A-Z rather than [X or Y]), the impact is minimized. Additionally, there is no *requirement* the government change the source or method information. They may well have decided to declassify the document. Although such action may be seen as unlikely, it should be sufficient to offset any gains the hostile organization makes by having the modified documents.

element to suspect a human source rather than an electronic one. As the risk of asset betrayal decreases it follows that the information flow would increase.

2. *Benefits to the Government*

While this paper attempts to alleviate a problem related to defenses in national security cases, it is also beneficial for the government. The government gets another method for transmitting information to the accused. As with other methods, this protects sensitive national security information by not revealing it to those without clearance. This allows for prosecutions based on classified information which, without source/method modified information, may otherwise be impossible and leave only more costly or otherwise suboptimal solutions.[130] There is a distinct advantage to using source/method modified information however in that it decreases the probability of leaks and intelligence assets being compromised in a number of ways.

One reason the government may be concerned with using classified data in the court systems is the fear that the information will get out. As discussed previously, there are multiple paths through which this may occur.[131] Before exploring two of these paths in more depth, an additional distinction may be valuable: information may be released by either an individual or a security flaw. Though using source/method modified information does not render the original information inherently more secure from things like network security flaws,[132] analysis of the aforementioned paths demonstrates the material is less likely to be released through individuals than in the status quo.

The first path for information to be released was through the defendant themselves. The government may fear that information could be elicited from counsel or documents which would reveal a source or

130. As discussed in Part I, if a defendant does not receive sufficient information the case cannot go to trial as it would be a violation of Article 5 of the European Convention on Human Rights or a similar rule. Eur. Convention on H. R. 5.4. The suspect may still pose a threat, however, prompting the government to undertake alternate arrangements to ensure he or she is not an active threat.

131. *See supra* Part I.C.

132. There are a host of possible electronic security flaws that could lead to intelligence being compromised, including unintended electrical emanations, referred to as TEMPEST. This leads to complicated restrictions and studies of hardware. *TEMPEST Certification Program*, NATIONAL SECURITY AGENCY (June 11, 2009), http://www.nsa.gov/applications/ia/tempest/index.cfm (describing the US program and providing lists of approved hardware); NATO INFORMATION ASSURANCE TECHNICAL CENTRE, http://www.infosec.nato.int/ (last visited Mar. 31, 2013) (including an overview of the NATO programs and lists of approved technology).

method.[133] Using modified information does not eliminate this concern, but it does alleviate it. By suggesting a plausible alternative story, the defendant may be less inclined or able to figure out how the information was obtained.[134] The government could presumably use any number of techniques to ensure the defendant does not derive the true source, from priming[135] to using other intelligence information to help craft the source/method modified information.[136]

Leaks to media or press, another path previously identified, are also less likely with source/method modified information. Journalists or other benign information seekers are less likely to pursue the unmodified information as the substance of the information will be the same. The distinction will be sources and methods—types of information journalists know are dangerous and, in some cases, illegal to publish.[137] The difference between the original and modified information also may not be meaningful to the media as they would still be able to report on the substance of the government's accusations. Accordingly, they may not proactively pursue the unaltered information. Additionally, those who transmit information to the media may be less inclined to do so when source/method modified information is available. When the only information available is extremely limited, individuals may feel that the public has a right to know the information in question and release the documents hoping to relay the substance of the allegations

133. This was the risk that the suspect would be "able to deduce . . . that certain places are being watched, or certain communications are being listened to." HOME AFFAIRS COMMITTEE, *supra* note 83.

134. If the government uses a weighing mechanism to determine when information is released, this should also mean more information will be released. I assume the calculus is something like: If ((*P*robability of sensitive information being compromised) x (*H*arm if revealed) > (*B*enefit to using information at trial), do not release. Or, release if (PxH) < B. Thus anything that decreases the probability of compromise or the harm to sources if revealed should increase the amount of information released to the defendant.

135. Priming is a psychology concept concerning the association of words and concepts. There are numerous studies demonstrating that an individual may be led to a certain concept or word based on how information is presented to them. See *What is Priming?*, PSYCHOLOGY TODAY, http://www.psychologytoday.com/basics/priming (last visited Mar. 31, 2013) for a more complete definition of priming, and *How Priming Impacts Your Performance*, YOUTUBE (June 3, 2011), http://www.youtube.com/watch?v=Z_mVFPCaQJY, for an interview with author Malcolm Gladwell discussing some of these studies in lay terms.

136. For example, if the intelligence community knew that a hostile organization was suspicious of a nonexistent human mole, they could model the source/method modified information on the fictional source, something the accused would be likely to believe (if, in fact, they are a member of the organization).

137. *See, e.g.*, 50 U.S.C. § 421 (making it illegal to publish certain intelligence source information).

to the public and inadvertently reveal sources and methods.[138] Having more complete substance available, even with modified sources, may ameliorate the notion that the public need to know is great enough to justify a leak.

Though it is true that foreign elements will know that modified information is allowed and thus may not trust information from the courts, this may still provide a benefit. First, it may be possible to structure the information in such a way that it is particularly believable, or, at a minimum, requires hostile counterintelligence to expend resources confirming the status either way. Second, this would remove the current certainty from the system. Until source/method modified information or something similar is allowed, a leak from a court that reveals a source or method can be presumed accurate. If this is no longer the case, the mere possibility of misinformation may confound the hostile element from confirming sensitive information.[139] Taken to its logical extreme, this means that even if source/method modified information were never used, simply having the option on the books may both benefit the government and increase the amount of information the government would be willing to reveal. The government may feel that the mere fact that the information *could* be modified or intentional misinformation[140] is enough to throw off hostile counterintelligence and thus cause information to be released in borderline cases.[141]

---

138. One possible example of this is Cheslea Manning providing classified documents to the WikiLeaks organization. Charlie Savage, *Soldier Admits Providing Files to WikiLeaks*, N.Y. TIMES, Mar. 1, 2013, at A1 (quoting Manning's desire to spark a policy debate and inform the public). Another is Edward Snowden leaking alleged National Security Agency (NSA) documents regarding electronic surveillance. Glenn Greenwald et al., *Edward Snowden: The Whistleblower Behind the NSA Surveillance Revelations*, GUARDIAN (June 9, 2013), http://www.guardian.co.uk/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance (quoting her as saying, "my sole motive is to inform the public").

139. *See supra* note 129 and accompanying text.

140. Governments may also wish to use source/method modified information to buttress ongoing disinformation campaigns or mislead enemy counterintelligence elements. That is, while the information may appear to simply disguise a source in court documents, it may be used by the government to "confirm" misinformation they have already transmitted to foreign entities. This obviously leads to complicated issues and harks back to the role of the judiciary in this process. Nonetheless, it is worth noting that such strategic modification may be possible and, if judicially or legislatively allowed, could create an additional incentive for the government to use source/method modified information.

141. By adjusting the assumed truth value of documents coming out of court, the government decreases the probability of sensitive information being compromised and therefore increases the pool of information they are able/willing to reveal. *See supra* note 134 (explaining a possible framework for government decision making that would lead to such an outcome).

3. Benefits to the Public:

Though not the intended beneficiary of this policy, the public may benefit as well. Counter-intuitively, allowing source/method modified information may increase public knowledge and understanding of intelligence operations and methods. Currently, it is unlikely source/method information will be publically available in any form. Information either will not be disseminated at all or will be heavily redacted. This leaves little more than Hollywood renditions of intelligence operations to inform the public.

Source/method modified information remedies this problem by revealing sources and methods, even if they are not depictions of the actual sources or methods used in the specific instance. By creating an alternative source or method the government is presumably creating a model for a reasonable or realistic intelligence operation. This may bridge any gap in understanding between the public and intelligence communities. This is because the substitute statements present a "story truth"—a facsimile that is likely to be internally consistent and perhaps truer even than a description of what actually took place. These are narratives that while not true in a technical sense, nonetheless relay a truth. There is a notion that "story-truth is truer sometimes than happening-truth."[142] Indeed, within the realm of literature, there is extensive scholarship about the function of truth in fiction.[143] The idea of story truth is that there are cases in which a literal recitation of the facts is insufficient to relay certain truths, which may be relayed with the aid of fiction.[144]

A similar idea exists in philosophy. Karl Popper famously wrote about verisimilitude, the concept that false theories may bear degrees of resemblance to truth.[145] For example, there is a long history of scientific theories being incorrect. Nonetheless, some of these incorrect theories are truer than others. The original model of the atom for example, may have been incorrect but contains far more truth than does

142. TIM O'BRIEN, THE THINGS THEY CARRIED 179 (1990).

143. *See, e.g.,* David Lewis, *Truth in Fiction*, 15 AMERICAN PHILOSOPHICAL QUARTERLY 37, 37–40 (1978) (arguing that statements within fiction can be 'true').

144. *Transcript of Conversation with Tim O'Brien*, NATIONAL ENDOWMENT FOR THE ARTS, http://www.nea.gov/av/avCMS/Obrien-podcast-transcript.html (last visited Mar. 31, 2013).

145. Karl Popper, *A Note on Verisimilitude*, 27 BRIT. J. FOR PHILOSOPHY OF SCI., No. 2, 47 (1976).

the ancient Greek concept of the five elements.[146] Popper explained that we develop, and accept the use of, false theories regularly.[147]

Regardless of the field of study, the application is the same in this case. Given the nature of intelligence, the full and complete account of the information simply will not be revealed. Even if the government revealed everything it possessed, this still may be inaccurate or incomplete. The government may have made judgment calls or may have unknowingly received misinformation. Any number of factors may complicate the government's most honest rendition of reality. That is all assuming the information would be revealed. Realistically, the very fact the information is classified is indication the government will not release it to the public.[148] Lacking omniscience, the public is essentially choosing between two non-true versions of the information—the source/method modified information or whatever limited, redacted, information comes from the other processes. Intelligence is thus like a world with only fiction or scientific theories that cannot be tested—absolute and complete truth is unavailable.

The question then is which of the two is more likely to be representative of the truth of intelligence operations. The source/method modified information will likely be internally consistent and representative of typical intelligence operations as they are being expressly created with the knowledge they will be public.[149] The sources and methods that were actually used may be fringe cases or, more likely, the information will simply not be available. It seems to follow that source/method modified information, which says something about intelligence operations, will more closely relay the truth than would silence on the government's behalf.[150] To the degree that truth is

146. Popper made similar arguments and wrote extensively about verisimilitude within the realm of science. *See*, G.S. Robinson, *Popper's Verisimilitude*, 31 ANALYSIS 194, 194 (1971).

147. "[F]alse theories often serve well enough: most formulae used in engineering or navigation are known to be false, although they may be excellent approximations and easy to handle; and they are used with confidence by people who know them to be false." KARL POPPER, SCIENCE: CONJECTURES AND REFUTATIONS, at X (1963).

148. Exec. Order No. 13,526 1.2(a)(1)-(3), 75 Fed. Reg. 707 (Dec. 29, 2009) (defining information in various classifications as damaging to national security if released).

149. Additionally, there should be external review and approval of these documents. *See infra* Part II.E.

150. One can imagine that if source/method modified information continually referenced pervasive electronic monitoring the public would have been able to consider and debate the proper scope and role of electronic surveillance in reasonable detail without Edward Snowden's leaks. *See* Eugene Robinson, Opinion, *Edward Snowden's NSA Leaks Show We Need a Debate*, WASH. POST (June 10, 2013), *available at* http://articles.washingtonpost.com/2013-06-10/opinions/39871061_1_oversight-foreign-intelligence-surveillance-court-intelligence-committees.

beneficial for the public, for example, to allow public debate of intelligence methods or properly allocate budgets, source/method modified information would thus provide a benefit.

There is reason to believe that publically accessible information about intelligence operations generally is beneficial. For example, after Edward Snowden leaked detailed information regarding alleged government surveillance programs[151] there was increasing skepticism about the role of government surveillance[152]—for the first time since the question was first asked in 2004, a plurality expressed greater concerns about civil liberties than security.[153] The incident also led members of Congress to propose an amendment limiting the NSA's surveillance powers.[154] Though this was narrowly defeated,[155] it indicates that public knowledge of intelligence programs may impact legislation. By having story truths in source/method modified documents, the public will be better able to understand the types of intelligence operations undertaken and the information that may be derived from those methods. Just as there was a public backlash after the Snowden leaks, there could be backlash to methods discussed in source/method modified information. Even if those methods were not and have not been used, such a backlash would still serve a signaling function to indicate to legislators and the intelligence community what methods would be deemed unacceptable in the eyes of the public. That is all to say so long as there is sufficient verisimilitude, the modified sources and methods provide the checks that come along with public disclosure without the current corollary, leaks.

E. Judicial Involvement

Before continuing, it is important to note that this process would not operate without judicial checks. As aforementioned, judges and cleared counsel or Special Advocates have access to the actual classi-

151. *See id.*

152. *Few See Adequate Limits on NSA Surveillance Program*, PEW RESEARCH (July 26, 2013), http://www.people-press.org/2013/07/26/few-see-adequate-limits-on-nsa-surveillance-program/.

153. *Id.*

154. *Amash SNSA Amendment Fact Sheet*, U.S. REP. JUSTIN AMASH (July 24, 2013), http://amash.house.gov/speech/amash-nsa-amendment-fact-sheet.

155. House Clerk, *Final Vote Results for Roll Call 412*, U.S. House of Representatives (July 24, 2013), http://clerk.house.gov/evs/2013/roll412.xml. However, the impact of Snowden's disclosures has not been fully determined. Though the Amash Amendment was defeated, this has not halted calls for reform and limitations on NSA's surveillance authorities. *See, e.g.*, USA Freedom Act, S. 1599, 113th Cong. (2013).

fied data.[156] I do not propose that this access be changed. This is true regardless of if source/method modified information is seen as a form of redaction or something unique.[157] Further, the use of source/method modified information would likely need to be tempered by additional or modified proceedings to fit within accepted bounds of fairness. In both CIPA and the Special Advocate system, a framework for proceedings of this nature already exist.

A potential danger of using source/method modified information is that accusations may appear stronger to a defendant than in fact they are. That is, perhaps the government classified information is based on a somewhat questionable human source but the source/method modified information makes it appear to be based on emails or phone records. This may prompt the accused to accept plea deals or mount subpar defenses if they believe their situation hopeless.[158] There is already extensive scholarship on the "innocence problem," the possibility that innocent defendants will plead guilty to crimes they did not in fact commit.[159] Indeed, approximately twenty percent of exonerees confessed to the crimes they did not commit.[160] This risk may be, in part, due to the accused not having full access to the evidence against them or feeling the evidence is strong.[161] Though source/modified information would be distinct from mechanisms in the traditional criminal system, the same conceptual concern of evidence appearing too strong would still apply. Accordingly, there should be systems in

156. *See supra* Part I.

157. Categorizing source/method modified information as a form of redaction or as a category unto itself would likely have a large impact on the implementation of such a procedure. Given that the Special Advocate system and CIPA currently allow for redaction, if source/method modified information is treated as redaction it could theoretically be utilized without legislative action. If distinct however, minor changes to legislation may be required. This paper intentionally left out details of implementation because as the procedure can be made to fit within a number of existing legal frameworks and explaining implementation in each did not seem efficacious.

158. There are multiple reasons that innocent defendants may choose to plead guilty to crimes they did not commit. *See* Lee Sorokin, *Why do Innocent People Plead Guilty?*, HUFFINGTON POST (May 29, 2012), http://www.huffingtonpost.com/judge-h-lee-sarokin/innocent-people-guilty-pleas_b_1553239.html.

159. *See generally* Lucian Dervan and Vanessa Edkins, *The Innocent Defendant's Dilemma: An Innovative Empirical Study of Plea Bargaining's Innocence Problem*, 103 J. CRIM. L. & CRIMINOLOGY 1 (2012).

160. Sorokin, *supra* note 158.

161. There is evidence that some defendants take pleas when the evidence appears to be strong, even if it is actually fabricated. Alexandra Natapoff, *At Least Five Imprisoned Based on lying Drug Informant*, SNITCHING BLOG (June 11, 2010, 4:08 PM), http://www.snitching.org/2010/06/at_least_five_imprisoned_based.html (discussing the case of Romill Blandin who pled guilty when confronted with informant fabricated evidence as well as several similar cases).

place to ensure the modified information does not appear stronger than the true source. This may take any number of forms from sua sponte decisions to motions by Special Advocates.

This leads to another potential issue. Typically, there is a remedy available if the prosecution crosses certain boundaries. Due to the evidence being in an open record, defendants can continue to challenge or examine the evidence against them, seeking exoneration or damages if it was fabricated.[162] Not only would this framework no longer function in the realm of source/method modified information, but there would likely be difficulty enforcing whatever parallel regulations may be created. This is because the classified information is likely to remain classified and thus cannot be reviewed by the accused, public, or academic communities. As a result, there may be no framework for utilizing *ex post* remedies if there is government misuse of source/method modified information, such as making evidence appear stronger than it actually is.[163] As a result, it makes sense to use *ex ante* systems to ensure there is fairness and avoid putting undue pressure on the accused. Both the Special Advocate system and CIPA already have mechanisms for closed hearings regarding classified information. These proceedings could be used to ensure there is judicial review of source/method modified information. Further, adversarial proceedings could be created wherein the Special Advocate or cleared counsel represented the interests of the accused in ensuring both that the substance of the original classified information was relayed and that the source/method modified information was not presented as stronger than the actual information.

III
Weighing the Costs of Source/Method Modified Information

Though source/method modified information provides an increased opportunity of transmitting information to the defendant and

162. Not only is exoneration possible, but damages can be recovered from government officials in some circumstances. *See* Buckley v. Fitzsimmons, 509 U.S. 259 (1993) (holding that prosecutors may be liable for certain actions); Monell v. Dep't of Soc. Servs., 436 U.S. 658 (1978) (holding that municipal corporations may be liable); Bivens v. Six Unknown Named Agents of Fed. Bureau of Narcotics, 403 U.S. 388 (1971) (holding that there are circumstances in which law enforcement officers may be liable for rights violations).

163. Even if the actual information is leaked, it may not be possible to use this information as the government may not confirm or deny even leaked information.

may be cabined by the judiciary,[164] the consequences of implementing such an institutional change have not been explored thus far. In determining if source/method modified information is to be utilized it is essential to understand both the sphere in which it could be used and the potential drawbacks of implementing such a change. This allows for weighing the costs and benefits of such a change. There are a number of factors to consider. The first is that there may still be information that cannot be transmitted, even when modified. This means that source/method modified information would not fully remedy the problems raised earlier.[165] There are also two potential drawbacks from implementing source/method modified information. First, allowing modification may be dangerous as it corrupts truth and, in doing so, leads to inaccurate outcomes. Second, this could alter public perception of the judiciary, at least in the national security context. These are both serious concerns to be examined and weighed against the benefits of source/method modified information.

There are a few situations in which modifying information would confer no benefit on the government or defendant. First, the intelligence information may be constrained to a very small number of people. By revealing that the government knows this information in any form, the leak could be traced to those people.[166] Similarly, if information was transmitted in only one fashion, misinformation as to method would be of no benefit as hostile counterintelligence would know the method of transmission regardless of modification.[167]

This would be particularly grave if the information the government was seeking to modify was coterminous with the types of information described above. There is reason to think this is not the case however. If it were, it would not be possible to use redaction or summarization of information as these too could be traced to a small cell of people or specific means of transmission. The fact that the government can use redacted documents, gists, or similar methods indicates that there is a pool of information in which the sensitive material can

164. *See supra* Part II.D.1 (discussing the benefits to defendants of using source/method modified information); *supra* Part II.E (discussing the role of the judiciary in the proposed process).

165. *See supra* Part I.C.

166. For example, if only three people knew a piece of information, no level of modification would relieve hostile CI scrutiny from those three people if the substance of that information were released.

167. Additionally, the government could not claim to have, say, satellite evidence of a discussion about intent that took place only via telephone. Revealing the substance of that conversation necessarily limits the method of obtaining information to the phone or one of the parties on the call.

be separated from at least some of the substance of the allegations. In situations where information is extremely constrained, either with regard to potential sources or methods, government may nonetheless be able to release more information when source/modified information is allowed. There are two reasons for this. First, in marginal cases the fact that any leak would not be de facto confirmation of the source or method could potentially alter the calculus to release information. That is, it may not even be necessary to use source/method modified information to reap the benefits of allowing it.[168] Second, it may still be possible to use source/method modified information as in the example of a faked raid. In those situations the fact that the information was extremely limited does not mean source/method modified information cannot convincingly look like one of the few other options.[169]

Additionally, a number of the benefits presented presume that source/method modified information will allow for increased communication between Special Advocates or cleared counsel and defendants. This is not necessarily the case, however. The same fear that currently prohibits cleared counsel or Special Advocates from speaking to defendants will still exist—it may be possible for the suspect to gather information from the lawyer without the lawyer being aware. Inadvertent disclosure to the accused may be due to a simple mistake or elicitation from the suspect. In either case, if the risk of the actual information being disclosed is too high, some of the key benefits will be nullified.

Source/method modified information may also be problematic because it goes against the idea of courts as bastions of truth, where people have taken a solemn oath to testify truly.[170] The integrity of the courts may thus be compromised if such methods were commonly used. This is linked to the potential criticism that accurate disposition of a case requires accurate information.[171] As inaccuracies in information increase, the probability of a correct outcome is likely to decrease.

---

168. *See supra* note 141. There is also the potential that if misinformation is allowed the misinformation benefits, or the widespread belief that the government uses misinformation, would outweigh the cost of releasing the information. Additionally, it may allow them to simply release more information as hostile elements would believe the information to be *intentionally* released, for example to frame one of their members as a spy while the defendant would benefit from the true information contained within the released documents. *See supra* note 140.

169. *See supra* Part II.B.

170. *See* FED. R. EVID. 603 (requiring a witness to "give an oath or affirmation to testify truthfully").

171. *See* Susan Haack, *Truth, Truths, "Truth," and "Truths*," 26 HARV. J. L. & PUB. POL'Y 17 (2003) (criticizing the idea of relative truth in courts). Additionally, this may explain rules against perjury and similar doctrines.

The fact that truth is explicitly corrupted in source/method modified information would thus mean that the court cannot fulfill its truth seeking function properly.

While the role of truth in the judicial system is certainly grounds for interesting scholarship, it may not be an applicable criticism in this context. First, the modified information is for the defendant and public—judges and cleared counsel, advocates or otherwise, still have access to the full information and thus may argue the unmodified information in an adversarial manner. Though it is true that this is still suboptimal, as the accused does not have full access to the information or counsel, utilizing this method likely presents them with more information and a greater ability to communicate than does the status quo. Additionally, it is not clear where the line would have to be drawn. Redaction is a form of limiting the complete truth and is used throughout the justice system, not merely in the context of national security.[172]

Further, it may not be the case that intelligence sources and methods are essential to a truth seeking venture. In his book *Obama's Wars*, Bob Woodward writes about an internal CIA practice regarding human sources much like source/method modified information:

> The CIA is so guarded with human sources that each one has a randomly selected code name such as MOONRISE. If the source is productive and undertaking great risks, word might get around the agency. He's doing great, but when too many people know about him he is killed off. There is a burial ceremony, everybody's sad. MOONRISE paid the ultimate price, his CIA case officer would say. Except MOONRISE is not actually dead. His code name has changed. And now the CIA has another source called SHOOTING STAR. It's an elaborate and manipulative ruse in order to grant MOONRISE the ultimate protection—death.[173]

If this account is accurate, the CIA uses source modified information *on itself*. By faking the death of a source they ensure the information being received is not degraded but protect the identity of the source by creating a false narrative of his/her life. This is important because if it is truly a CIA practice, it demonstrates that source/method modified information has been used in agencies seeking to learn accurate information. Presumably the quality of intelligence assessments did not appreciably degrade or such a practice would be abandoned or scrapped in early phases of implementation. If CIA

172. *Supra* Part II.C (discussing redaction of the names of minors, police informants or undercover officers, and personal identifying information).

173. BOB WOODWARD, OBAMA'S WARS, 6–7 (2010).

practices demonstrate that source information can be modified and still used accurately in intelligence assessments, it seems likely that they could be used to generate similarly accurate information in courts, which have greater procedural protections, an appeals process, and multiple adversarial parties who have seen the unmodified information. It may still be possible to distinguish these situations however. Things coming from courts are presumed to be true and transparent. When there is redaction, this is clear. CIA practitioners are likely trained at distilling information and dealing with misinformation. While they may be able to make assessments with modified information, it does not necessarily follow that the judicial system could seamlessly do the same. Further inquiry and discussion with those familiar with the CIA practice would be required to properly assess the impact this would have on courts.

It is also beneficial to consider the truth of these documents in another light: the interaction of truth and justice, particularly in extraordinary circumstances. Scholarship surrounding truth and reconciliation committees highlights this. There is an idea of "truth versus justice," that traditional notions of justice may not be compatible with truth-seeking ventures in all circumstances.[174] Indeed, in seeking truth such commissions "sacrifice the pursuit of justice as usually understood."[175] Nonetheless, proponents argue that there is a form of justice[176] that is nonetheless achieved through these processes and truth, necessary for these societies, is uncovered.[177] That is, in certain circumstances we may prioritize truth over traditional justice and take a different notion of justice in its stead. Source/method modified information is the inverse position, that to create more justice in the system a degree of truth is sacrificed. As with truth and reconciliation committees not wholly sacrificing the idea of justice, source/method modified information does not wholly sacrifice truth.[178] It retains a measure

174. This discussion arises in the context of truth and reconciliation committees. *See*, TRUTH V. JUSTICE: THE MORALITY OF TRUTH COMMISSIONS 3–45 (Robert I. Rotberg & Dennis Thompson eds., 2000).

175. *Id.* at 8.

176. This is typically referred to as "restorative justice" or "transitional justice." *See* Erin Daly, *Transformative Justice: Charting a Path to Reconciliation*, 12 INT'L LEGAL PERSP. 73 (2002).

177. Paul Lansing & Julie C. King, *South Africa's Truth And Reconciliation Commission: The Conflict Between Individual Justice And National Healing In The Post-Apartheid Age*, 15 ARIZ. J. INT'L & COMP. L. 753, 782–84 (1998) (discussing how "healing" may occur with truth).

178. The truth value in this instance is "story truth." Regardless of if one believes it to be a close proxy for happening truth, or even more accurate in some manner of speaking, it is *a* truth value. More to the point, the "truth versus justice" discussion

of truth but recognizes that for the accused, having access to information is paramount.

Yet another potential criticism is that if the public believes that the courts are no longer in the service of truth but instead a vehicle for the government's security interests, they may lose faith in the independence or value of the judiciary. Currently, the court serves as a legitimizing function for intelligence operations. For example, public polls regarding NSA surveillance after the Snowden leaks showed a twelve percent increase in support of the surveillance if done with court approval.[179] This was an increase of nearly fifty percent as compared to those who were not told anything about the involvement of the courts.[180] If the courts are seen as linked to manipulating information on the government's behalf, there is a risk that the public perception of legitimization will disappear.

There is an interesting tension however, because while the public's response to surveillance was heavily influenced by discussion of court involvement, the majority of Americans polled did not believe the courts provided adequate limits on information collected by the NSA.[181] Additionally, to properly assess this argument, source/method modified information must be seen within the larger institutional framework for counterterror and counterintelligence operations. Not only are there doctrines and pieces of legislation specifically created for national security information such as CIPA or the Special Advocate systems, but preexisting court decisions may already lead those so inclined to such beliefs. In the U.S. for example, cases dismissed on standing grounds[182] or due to the state secrets doctrine[183] may lead to similar criticisms.[184] This is not however, necessarily a strong argument against utilizing those doctrines. Nonetheless, there does appear to be statistically significant evidence that the public is

---

may create an equation of sorts wherein high values of truth make up for low levels of justice. If these are pegged however, increasing the justice inherent in the system may allow for explicitly less truth using the same logic.

179. *Government Surveillance: A Question Wording Experiment, Pew Research* (July, 26 2013), http://www.people-press.org/2013/07/26/government-surveillance-a-question-wording-experiment/.

180. 37% favored if told there was court approval, 25% if there was no mention of the court. *Id.*

181. *Few See Adequate Limits on NSA Surveillance Program*, *supra* note 152.

182. *See, e.g.*, Al-Aulaqi v. Obama, 727 F. Supp. 2d 1 (D.C. Cir. 2010).

183. *See* United States v. Reynolds, 345 U.S. 1 (1953). There are also recent cases dismissed on "state secrets" grounds. *See* Mohamed v. Jeppesen Dataplan, Inc., 614 F.3d 1070 (9th Cir. 2010).

184. *Obama Dishes Up A Cup Of Same Old Same Old,* DAILY KOS (Feb. 10, 2009, 2:39 PM), http://www.dailykos.com/story/2009/2/10/173636/600/828/695835. *See also*, Robinson *supra* note 150.

currently more likely to find collection acceptable if approved by the court. If the court is seen not simply as being inadequate in a certain case, but actively supporting the security apparatus, that perception of judicial legitimacy may be lost.

This leads to a number of thoughts. First, the risk of public belief that the judiciary is biased has to be balanced against the benefits of undertaking the action in question. Whatever harms come from a distrustful public must be weighed against the benefits to the parties at hand. Second, public perception of policies may speak more to how they were presented than their merits. If source/method modified information would have the benefits described in Part II but the public seems skeptical, it may be that the public merely needs to be better informed of the benefits, particularly those to the defense. Finally, those who believe the courts are beholden to the government in national security cases may well believe this is true due to court decisions allowing extensive NSA surveillance, on standing grounds, control order jurisprudence, or any other court actions in favor of the government.

Yet another potential criticism is that much of the power of source/method modified information is lost when its use is public. The problem is not using source/method modified information, but admitting to using it. The benefits to misinformation, for example,[185] are lost at the point that hostile elements know that the information is, or may be, false. None of the benefits of source/method modified information would be lost if such a policy were pursued in secret. To the contrary, some would be magnified. Depending on how secret this policy was, there may even be additional benefits. For example, if information were modified and then shown to a Special Advocate, the government may be willing to allow extensive communication between the advocate and the accused.

Having the source/method modified information policy be public and subject to review seeks to provide a balance. Complete secrecy doesn't seem to allow for judicial oversight or a strong adversarial process. It thus may violate the right to a fair trial or the modified information may push defendants to accept plea bargains.[186] There may however, be space for partial secrecy—allowing for source/method modified information but keeping that from the general public. In such a system, the judges and counsel would be involved but the full details of policy would not be public. This, however, is an

185. *See supra* notes 140–41 and accompanying text.

186. *See supra* Part II.E.

alternate method of implementation more than a criticism of using source/method modified information.

These are very real and very valid criticisms. This paper rests on assumptions about increasing the flow of information and the impact a policy of this nature would have on the government during litigation. If experience or further research found these to be false, a policy of this nature may do little more than undermine public confidence. However, these criticisms, while valid, tend to be general in nature. That is, they are more the product of the tension inherent in judicial processes involving classified information than they are (for the most part) criticism of this system specifically. The idea that the public may lose faith in the judicial system and see it beholden to the government, for example, is something that could be said of any special protection given to classified information. Similarly, the fact that this may not always enable more information to be provided to the defendant could be said of redaction, anonymization, or other methods of protecting sensitive information. It is true that there are categories of information for which this form of protection will be inadequate. This too is true of redaction.

The costs and benefits of source/method modified information cannot be properly assessed in a vacuum. Instead, it is imperative that they be compared to the alternatives available. If, for example, one wishes to set the procedural protections and disclosure requirements very high in these cases, it must be asked if it is better to have the government never bring the suspect to trial at all and instead mount an intensive surveillance operation or, if possible, deport the suspect for pretextual reasons. If concerned about the quality of information reaching the accused, one cannot look at typical criminal trials but instead must compare it to the framework that would actually be used—the heavy redactions present in the CIPA or Special Advocate systems. Source/method modified information is not the solution to all cases and is not applicable in all situations. Nonetheless, it may well be beneficial in some situations with some forms of information even though these benefits likely come at some cost to the judiciary.

CONCLUSION

There is no telling precisely how or when source/method modified information would be used. Such decisions would undoubtedly be fact dependent and made by those with access to classified data. It seems highly plausible however, that there could be more trials. Governments would be more able to introduce evidence and witnesses without offending their respective laws. This may be better for people

in situations like Mohamad's.[187] While undoubtedly source/method modified information would not have prevented the practice of extraordinary rendition, it does open up the possibility of using the legal process where it may otherwise be unavailable. It seems reasonable to assume that measures such as extraordinary rendition are undertaken when less restrictive means, such as trials, are unavailable. Bringing those like Mohamad into the legal system rather than sending them to ill-treatment in the Middle East is undoubtedly beneficial for defendants.

Those are, of course, fringe cases. The benefits of source/method modified information go beyond channeling more suspects into the courtroom; they also make the process within the courtroom a fairer one. Defendants like those in *A v. United Kingdom*[188] would be able to challenge the allegations against them in a more meaningful way.

Central among criticisms of both CIPA and the Special Advocate system are that defendants cannot meaningfully participate in their own litigation due to the existence of the classified materials. Currently, defendants often have only pieces of the pertinent information and limited access to counsel. This is because while the defendant has an interest in the fairness of the trial, governments have a countervailing interest in maintaining the secrecy of national security information at trial. This has historically led to legislation attempting to split the difference, making some concessions for fairer trials and others for protection of sensitive materials.

A tradeoff may not always be required. If the information that the government is seeking to protect is not the information that is of value to the defendant, legislatures or courts only need create a system that enables the sensitive information to be stripped from the pertinent substantive information. This allows for defendants, like A, to mount a more meaningful defense while ensuring the sensitive materials are protected from disclosure.

While it is impossible to determine precisely what information would have been available to A and the others if source/method modified information had been used, or, indeed, if Mohamad would have been subject to extraordinary rendition, this proposal does not seek to fully solve the legal complications of using classified information at trial. It certainly does not attempt to address the legality or wisdom of particular intelligence operations. Instead, it aims to create another avenue for possible information flow. Such a flow would be polyvalent,

187. Mohamed v. Jeppesen Dataplan, Inc., 563 F.3d 992 (9th Cir. 2009).
188. A v. United Kingdom, App. No. 3455/05, Eur. Ct. H.R. (2009).

benefitting not only the defendant but also the government and the public.

It is, however, essential to recognize not only the range of possible benefits but also potential institutional impacts of such a policy. Those with better access to information would likely be able to weigh the costs and benefits of source/method modified information in a way that simply cannot be done in an unclassified academic setting. As with other doctrines in the national security context, myopic thinking is dangerous. Policymakers would need to consider not only the potential benefits to those involved, but the legitimacy of the courts, the potential for misuse, and the role of the judiciary in the process.