Hijacking the Privilege: Balancing Fairness and Security When Warrantless Wiretapping Threatens Attorney-Client Communications

*William Wetmore**

Introduction

Shakir Baloch is a family doctor with a wife and a fifteen-year-old daughter.[1] A native of Pakistan from a politically prominent family that supports progressive secularism in that country, Baloch moved to Canada in 1989 and became a Canadian citizen in 1994.[2] In April 2001, he came to the United States to find work.[3] Shortly after the September 11, 2001 attacks, Baloch and several other Muslim men were arrested on immigration violations and transferred to the Metropolitan Detention Center ("MDC") in Brooklyn.[4] According to Baloch, he and the others were placed in MDC's Administrative Maximum Special Housing Unit ("ADMAX SHU") for more than twenty-three hours per day, where they were strip-searched, shackled when removed from their cells, and verbally and physically abused by prison guards for several months.[5]

After being cleared of terrorist links[6] and deported, Baloch and several other detainees sought justice in the U.S. civil litigation system for the harsh treatment they suffered while incarcerated in the MDC. In April 2002, the detainees filed a class-action suit in the United States District Court for the Eastern District of New York, making constitutional and federal tort claims against several high-ranking U.S. officials and prison personnel.[7]

While the case was ongoing, national media reported that the government had been conducting warrantless electronic surveillance of individuals

---

* J.D. Candidate, The George Washington University Law School, 2008. The author thanks Stephen Handler and Clay Mahaffey for their generous help in clarifying details about the post-September 11 detainee litigation, and Megan Murphy Wilcox and Marcy Busch for their excellent comments on drafts of this Essay.

[1] Third Am. Class Action Compl. and Demand for Jury Trial at 10, Turkmen v. Ashcroft, No. 02 CV 2307 (E.D.N.Y. Sept. 13, 2004).

[2] *Id.*

[3] *Id.*

[4] *Id.* at 2–4.

[5] *Id.* An investigation by the Office of the Inspector General of the U.S. Department of Justice substantiated many of the allegations by the ADMAX SHU detainees. *See generally* Office of the Inspector Gen., U.S. Dep't of Justice, The September 11 Detainees: A Review of the Treatment of Aliens Held on Immigration Charges in Connection with the Investigation of the September 11 Attacks (2003), *available at* http://www.usdoj.gov/oig/special/0306/full.pdf.

[6] Third Am. Class Action Compl. and Demand for Jury Trial, *supra* note 1, at 27.

[7] *Id.* at 1–8.

suspected of having links to terrorism.[8] The attorneys representing the post-September 11 detainee plaintiffs became concerned that the government would never be required to inform the plaintiffs whether they had been subject to such surveillance because the information could be protected by the state secrets privilege, which completely bars civil discovery when national security information is at issue.[9] The plaintiffs' attorneys feared that the government would use these confidential communications against their clients without their knowledge and without judicial scrutiny.[10]

This Essay will argue that in cases in which confidential attorney-client communications are threatened, courts should seek to balance the plaintiffs' concerns about prejudice with the government's legitimate national security interests. Courts should give limited deference to government assertions of the state secrets privilege in civil cases in which the plaintiffs' confidential attorney-client communications credibly could have been captured by a warrantless surveillance program.

Part I addresses the importance of attorney-client privilege in the U.S. civil litigation system, and how the National Security Agency ("NSA") surveillance program in question could chill confidential attorney-client communications. Part II examines the history of and justification for the state secrets privilege. Part III proposes that judges balance the concerns of the plaintiffs and the government using in camera, ex parte review of any intercepted attorney-client communications.

I. Attorney-Client Privilege and Warrantless Wiretapping

Attorneys' ability to hold open conversations with their clients is essential for preparing a case and has been recognized and highly valued by the Supreme Court.[11] The Court has stated that the privilege is one of the "oldest recognized privileges for confidential communications," and that it is intended to encourage "full and frank communication between attorneys and their clients and thereby promote broader public interests in the observance of law and the administration of justice."[12]

Warrantless wiretapping of suspected terrorists presents a significant threat to the attorney-client privilege. On December 16, 2005, the *New York Times* reported that the NSA had conducted warrantless electronic surveil-

---

[8] James Risen & Eric Lictblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. Times, Dec. 16, 2005, at A1.

[9] Pls.' Mem. in Opp'n to the United States' Objections to the Order of Magistrate Judge Gold Entered May 30, 2006 at 6–13, Turkmen v. Ashcroft, No. 02 CV 2307 (E.D.N.Y. 2006).

[10] *Id.*

[11] *See, e.g.*, Swidler & Berlin v. United States, 524 U.S. 399, 403–10 (1998); Upjohn Co. v. United States, 449 U.S. 383, 389–91 (1981); Chase Manhattan Bank v. Turner & Newall, PLC, 964 F.2d 159, 165 (2d Cir. 1992).

[12] *Swidler & Berlin*, 524 U.S. at 403 (quoting *Upjohn*, 449 U.S. at 389); *see also* Ellen S. Podgor & John Wesley Hall, *Government Surveillance of Attorney-Client Communications: Invoked in the Name of Fighting Terrorism*, 17 Geo. J. Legal Ethics, 145, 159 (2003).

lance of individuals suspected of being linked to terrorism.[13] According to the *Times*, President Bush issued a secret executive order in 2002 permitting the NSA to conduct the warrantless surveillance.[14] President Bush acknowledged and defended this program, known by the administration as the "Terrorist Surveillance Program" ("TSP"), as crucial for defending the country against further terrorist attacks.[15]

Although the administration stated in 2007 that it voluntarily ended the TSP, former Attorney General Alberto Gonzales reasserted that the TSP "fully complies with the law"[16] and did not foreclose the possibility that this or future administrations might conduct warrantless surveillance in a similar fashion.[17] As long as the Executive Branch insists that it can legally intercept communications without judicial scrutiny, plaintiffs cannot be assured that their attorney-client communications are confidential.

As a result, attorneys representing clients possibly subject to TSP or other warrantless surveillance programs may have to take extreme steps to avoid communications with their clients, or entirely avoid substantive communications with their clients.[18] This chilling effect creates severely prejudicial conditions for plaintiffs suing the government.[19] Attorneys facing these prejudicial conditions have moved courts to compel the government either to cease TSP surveillance or to disclose whether their clients were monitored.[20]

The plaintiffs in *Turkmen v. Ashcroft* and its companion case, *Elmaghraby v. Ashcroft*,[21] were detained pursuant to the federal investigation of the September 11 terrorist attacks.[22] After they were deported, they filed suit in federal court and communicated with their attorneys in the United

---

[13] James Risen & Eric Lictblau, *supra* note 8, at A1.

[14] *Id.*

[15] President George W. Bush, Press Conference (Dec. 19, 2005).

[16] David Stout, *Court Will Monitor Eavesdropping in U.S.; Shift by Bush Administration is Hailed*, INT'L HERALD TRIB., Jan. 19, 2007, at 3.

[17] Dan Eggen, *Court Will Oversee Wiretap Program: Change Does Not Settle Qualms About Privacy*, WASH. POST, Jan. 18, 2007, at A1.

[18] *See* ACLU v. NSA, 438 F. Supp. 2d 754, 767–68 (E.D. Mich. 2006) (finding that although the plaintiffs were "resorting to other 'inefficient' means for gathering information, the TSP continues to cause 'substantial and ongoing harm to the attorney-client relationships and legal representations' "), *vacated*, 493 F.3d 644 (6th Cir. 2007).

[19] *See* Turkmen v. Ashcroft, No. 02 CV 2307, 2006 WL 1517743, at *3–4 (E.D.N.Y. May 30, 2006) (recognizing that plaintiffs' effort to learn whether their conversations with their attorneys were monitored by the government "is not a mere fishing expedition based on unfounded speculation" and that information about surveillance of attorney-client communications is needed to assure that the "defendants have not gained a tactical advantage by invading the attorney-client privilege").

[20] *See*, *e.g.*, Hepting v. AT&T Corp., 439 F. Supp. 2d 974, 978–79 (N.D. Cal. 2006); Terkel v. AT&T Corp., 441 F. Supp. 2d. 899, 903 (N.D. Ill. 2006); ACLU v. NSA, 438 F. Supp. 2d at 770–71; Al-Haramain Islamic Found. v. Bush, 451 F. Supp. 2d 1215, 1218 (D. Or. 2006).

[21] Elmaghraby v. Ashcroft, No. 04 CV 1809 (E.D.N.Y. 2002).

[22] Third Am. Class Action Compl. and Demand for Jury Trial, *supra* note 1, at 2.

States.[23] Based on what is known about the TSP, these otherwise privileged communications could have been subject to TSP surveillance.[24]

The plaintiffs in *Turkmen* and *Elmaghraby* issued an interrogatory asking the government to confirm or deny whether their confidential communications had been intercepted.[25] The government refused to disclose this information. Although the state secrets privilege[26] was never formally invoked, the government's arguments were similar to those traditionally offered in support of an assertion of the privilege.[27]

A federal magistrate judge issued an order requiring disclosures by the government.[28] The government objected to the order and the matter was considered in federal district court, which ultimately agreed with the magistrate judge that "it is a cardinal rule of litigation that one side may not eavesdrop on the other's privileged attorney-client communications."[29] The district court stated that, "because of the unusual circumstances of this case, the plaintiffs' request for further assurance that the rule has not been violated in this case is reasonable."[30] The "unusual circumstances" to which the court referred were: 1) that the United States had claimed the authority to monitor suspected terrorists abroad making electronic communications into the United States without any judicial oversight; and 2) that the plaintiffs were detained in the United States for months under suspicion that they were involved in terrorist activity and thus were subjected to further interrogation when they returned to their home countries, leading them to believe that the United States requested the foreign authorities watch them.[31]

The court concluded that "regardless [of] whether the plaintiffs are actually involved in terrorist activity—they emphatically state that they are not—they have reason to believe that the government thinks they are, and that they are therefore being monitored when they call the United States."[32]

The plaintiffs' need to know whether their attorney-client communications were monitored, however, must be balanced with the government's interest in protecting classified information.[33] To protect the government's

---

[23] Turkmen v. Ashcroft, No. 02 CV 2307, 2006 WL 4483151, at *2 (E.D.N.Y. Oct. 3, 2006).

[24] *Id.* at *3; *see also Al-Haramain Islamic Found.*, 451 F. Supp. 2d at 1222–23.

[25] Turkmen v. Ashcroft, No. 02 CV 2307, 2006 WL 1517743, at *1 (E.D.N.Y. May 30, 2006) (requesting disclosure of "whether any telephone, email or other communication between any plaintiff and his counsel was monitored or intercepted since the plaintiff's removal from the United States").

[26] For a detailed discussion of the state secrets privilege acting as a bar to discovery in civil cases, see *infra* Part II.

[27] *See* Pls.' Mem. in Opp'n to the United States' Objections to the Order of Magistrate Judge Gold Entered May 30, 2006, *supra* note 9, at 25.

[28] *Turkmen*, 2006 WL 1517743, at *6.

[29] Turkmen v. Ashcroft, No. 02 CV 2307, 2006 WL 4483151, at *2 (E.D.N.Y. Oct. 3, 2006).

[30] *Id.* at *3.

[31] *Id.*

[32] *Id.*

[33] *Id.*

interest, the district court ordered the required disclosures by the government to be made ex parte for review in camera.[34] Specifically, it required the government to disclose "whether any defendant, any likely witness or any member of the trial team . . . has knowledge (or had knowledge in the past) of the substance of any intercepted confidential communications between the plaintiffs and their attorneys."[35]

Following the district court's ex parte, in camera review, the plaintiffs would be given either:

> (1) assurance by the Court that the United States' representation that no TSP intercepts of the plaintiffs will be used in the defense of this action has been fully substantiated, or (2) notice of any remedial action that has been taken and an opportunity to be heard as to the necessity of further measures.[36]

II. History of and Justification for the State Secrets Privilege

The state secrets privilege is well established and can be traced to English common law.[37] The government, with authorization from the head of the agency in question, can assert the privilege to block discovery in a lawsuit of any information whose disclosure would adversely affect national security.[38] After the agency head formally invokes the privilege, the court must determine whether the circumstances warrant the claim of privilege.[39] Courts must be careful in making this determination to avoid disclosure of the very information the privilege is designed to protect.[40]

The Court stated in *United States v. Nixon* that the state secrets privilege derives from the President's Article II authority to conduct foreign policy and provide for the national defense, and that in such matters the Court has traditionally "shown the utmost deference to Presidential responsibilities."[41]

---

[34] *Id.* at *5.

[35] *Id.*

[36] *Id.* at *6. On October 20, 2006, the court granted a motion by the United States to allow the government, through the NSA, to make a comprehensive submission of the requisite information. On December 6, 2006, the court entered an order stating: "The United States' representation that no Terrorist Surveillance Program ("TSP") interceptions of the plaintiffs will be used in the defense of this action has been fully substantiated." Turkmen v. Ashcroft, No. 02 CV 2307 (E.D.N.Y. Dec. 6, 2006). The court did not address whether the ruling would have been different had the United States formally invoked the state secrets privilege to prevent any disclosure of information related to the TSP.

[37] *See, e.g.*, United States v. Reynolds, 345 U.S. 1, 6–8 (1953).

[38] *Id.* (noting that the existence of the privilege had been conceded even by "the most outspoken critics of governmental claims to privilege").

[39] *Id.* at 8.

[40] *Id*.

[41] United States v. Nixon, 418 U.S. 683, 710 (1974).

Courts have not precisely defined national security.[42] The government has asserted the privilege to protect against disclosure of information regarding the nation's defense capabilities and intelligence-gathering methods or capabilities, and to avoid disruption of diplomatic relations with foreign governments.[43] Furthermore, courts have allowed the executive to invoke the privilege to prevent access to information in a particular case, despite past executive disclosure of similar information in other cases.[44]

When faced with civil discovery requests concerning classified surveillance programs, the government has stated in several cases that it can neither confirm nor deny who was subject to the programs.[45] The government has argued that simply confirming or denying that someone is subject to a classified surveillance program in one case but refusing to confirm or deny that fact in another case would reveal classified information.[46] This state secrets privilege justification has been labeled the "mosaic theory."[47]

This theory was outlined in *Halkin v. Helms*, in which the D.C. Circuit explained that simply informing a target that he or she was subject to surveillance "would enable foreign governments or organizations [with whom the target communicated] to extrapolate the focus and concerns of our nation's intelligence agencies."[48] The court further stated that it "requires little reflection to understand that the business of foreign intelligence gathering in this age of computer technology is more akin to the construction of a mosaic than it is to the management of a cloak and dagger affair."[49] Intelligence experts, the court explained, can weave together the thousands of "seemingly innocuous" pieces of revealed information to discover the larger objectives of American intelligence.[50]

---

[42] *See* New York Times v. United States, 403 U.S. 713, 739 (1971) (White, J., dissenting) (noting that "national defense" is a generic term not susceptible to precise definition); Ellsberg v. Mitchell, 709 F.2d 51, 57 (D.C. Cir. 1983) (noting that because the state secrets doctrine "pertains generally to *national security* concerns, the privilege has been viewed as both expansive and malleable"); *see also* Note, *The Military and State Secrets Privilege: Protection for the National Security or Immunity for the Executive?*, 91 YALE L.J. 570, 574 (1982).

[43] *Ellsberg*, 709 F.2d at 57.

[44] *See* Halkin v. Helms, 598 F.2d 1, 10 (D.C. Cir. 1978) ("The government is not estopped from concluding in one case that disclosure is permissible while in another case it is not."); *see also* Note, *supra* note 42, at 574.

[45] *See Halkin*, 598 F.2d at 1.

[46] *Id.*

[47] *See, e.g.*, Meredith Fuchs, *Judging Secrets: The Role Courts Should Play in Preventing Unnecessary Secrecy*, 58 ADMIN. L. REV. 131, 169 (2006); David E. Pozen, Note, *The Mosaic Theory, National Security, and the Freedom of Information Act*, 115 YALE L.J. 628, 640 (2005); Shannon Vibbert, Comment, *A Twisted Mosaic: The Ninth Circuit's Piecemeal Approval of Environmental Crime In* Kasza v. Browner, 17 J. NAT. RESOURCES & ENVTL. L. 95, 104 (2002–03).

[48] *Halkin*, 598 F.2d at 7.

[49] *Id.*

[50] *Id.*

III. Striking a Balance Between Liberty and Security

Protecting confidential communications between an attorney and his client is fundamental to ensuring fairness in our adversarial civil litigation system.[51] The mere possibility of warrantless surveillance threatens the viability of the attorney-client privilege for plaintiffs who sue the government.[52] If the government properly invokes the state secrets privilege concerning the classified nature of a warrantless surveillance program, and a judge accepts the assertion, the plaintiffs would never know whether their confidential communications were intercepted and being used against them in the government's case.

The government, however, has an urgent and legitimate interest in protecting classified national security information.[53] Requiring elements of classified intelligence programs to be revealed upon any discovery request in a civil suit could severely undermine such programs and the government's efforts to fight the continuing threat of international terrorism.[54] For this reason, a solution to this urgent problem must balance the plaintiffs' concerns about warrantless surveillance prejudicing their case with the government's legitimate national security interests.[55]

One solution lies in enhanced judicial scrutiny. Courts have a duty to "ensure that the state secrets privilege is asserted no more frequently and sweepingly than necessary," which requires that they "critically . . . examine" assertions of the privilege.[56]

In warrantless surveillance cases, courts have critically assessed state secrets assertions by reviewing government declarations and classified material in camera, ex parte.[57] Courts are required by statute to conduct such a review to determine whether the government undertook surveillance lawfully and pursuant to a warrant from the Foreign Intelligence Surveillance ("FISA") Court.[58] In *Ellsberg v. Mitchell*, the D.C. Circuit stated that courts

---

[51] *See* Swidler & Berlin v. United States, 524 U.S. 399, 403–10 (1998); Upjohn Co. v. United States, 449 U.S. 383, 389–91 (1981); Chase Manhattan Bank v. Turner & Newall, PLC, 964 F.2d 159, 165 (2d Cir. 1992); Part I, *supra*.

[52] *See* Turkmen v. Ashcroft, No. 02 CV 2307, 2006 WL 1517743, at *6 (E.D.N.Y. May 30, 2006).

[53] *See* Ellsberg v. Mitchell, 709 F.2d 51, 56 (D.C. Cir. 1983).

[54] *See Halkin*, 598 F.2d at 8.

[55] *See* Turkmen v. Ashcroft, No. 02 CV 2307, 2006 WL 4483151, at *2–3 (E.D.N.Y. Oct. 3, 2006).

[56] *Ellsberg*, 709 F.2d at 58.

[57] *See id.* at 54; Hepting v. AT&T Corp., 439 F. Supp. 2d 974, 978–79 (N.D. Cal. 2006); ACLU v. NSA, 438 F. Supp. 2d 754, 764 (E.D. Mich.), *vacated*, 493 F.3d 644 (6th Cir. 2007); Al-Haramain Islamic Found. v. Bush, 451 F. Supp. 2d 1215, 1219 (D. Or. 2006).

[58] *See* ACLU Found. Of S. Cal. v. Barr, 952 F.2d 457, 462 (D.C. Cir. 1991) (noting that, under 50 U.S.C. § 1806(f), "Federal district courts 'shall' conduct ex parte, in camera reviews to determine whether FISA surveillance, undertaken pursuant to an order of the FISA Court, was 'lawfully authorized and conducted' whenever the issue arises in a proceeding and the Attorney General, in an affidavit, represents that disclosure or an adversary hearing would harm the national security interests of the United States.").

should probe deeply into whether invoking the privilege is appropriate when a litigant can show a compelling need for the information.[59] By the same token, courts should give more deference to the government when disclosure could plausibly and substantially endanger national security.[60]

In cases where plaintiffs suing the government have reason to believe that the government used a warrantless surveillance program to monitor their attorney-client communications, the deference to national security that *Ellsberg* requires should be at its lowest ebb. To prevent limited disclosure, courts should require the government to give substantial and specific assurances through classified submissions that either the plaintiffs' attorney-client communications were not intercepted, or that the government will not use any such interceptions to defend the case.[61]

If the government makes a comprehensive and satisfactory submission, the court could issue an order similar to that in *Turkmen v. Ashcroft*, which assured the plaintiffs that the government would not use any interceptions in the case.[62] Although the *Turkmen* plaintiffs did not discover whether the government had intercepted their communications, they could at least be satisfied that a judge had scrutinized the government's submissions and concluded that no interceptions of privileged attorney-client communications would prejudice the case.

The government did not formally invoke the state secrets privilege in *Turkmen*, but in a case where the privilege is invoked, a judge could couple a similar order with a statement that it should not be interpreted as confirming or denying whether the government intercepted attorney-client communications.[63] The order would serve only as an indication that the judge was satisfied that the plaintiff's case would not be prejudiced. The judge could make this finding based either on assurances that the government would not use the intercepted communications improperly, or that the government had never intercepted any communications. The statement would provide no elaboration on the finding, and would therefore amount to neither confirmation nor denial that the government monitored a particular individual, thereby assuring the government that its classified mosaic would not be revealed.

If the government's submission did not satisfy the court, the judge could order further in camera, ex parte disclosures,[64] or limited disclosure to the

---

[59] *Ellsberg*, 709 F.2d at 58–59.

[60] *Id.*

[61] *See, e.g.*, Turkmen v. Ashcroft, No. 02 CV 2307, 2006 WL 4483151, at *3 (E.D.N.Y. Oct. 3, 2006).

[62] *Id.*; *see also supra* Part I.

[63] *See* Hepting v. AT&T Corp., 439 F. Supp. 2d 974, 994–95 (N.D. Cal. 2006) (stating that its ruling following its initial in camera, ex parte review should not be interpreted as confirming the truth of the plaintiffs' claims).

[64] *See* Al-Haramain Islamic Found. v. Bush, 451 F. Supp. 2d 1215, 1231 (D. Or. 2006) (stating that the court might require the government to give "specific responses to the [plaintiffs'] interrogatories for in camera, ex parte review").

plaintiffs.[65] In considering limited disclosure, courts should follow the *Ellsberg* court's mandate that "whenever possible, sensitive information must be disentangled from nonsensitive information to allow for the release of the latter."[66] Courts also should "take special care to honor the extraordinary security concerns raised by the government."[67] In *Al-Haramain Islamic Foundation v. Bush*, the court urged the government to consider redacting portions of a classified document to allow disclosure to the plaintiffs.[68] A judge could issue a similar instruction when the interception of confidential attorney-client information is at issue.

If the court ordered disclosure, the government likely would argue that their classified mosaic would be compromised regardless of the extent of redaction.[69] The court, however, could take innovative procedural measures to ensure that any information disclosed would not be vital to national security.[70] For example, the court might appoint a special master to help determine what information provided during in camera, ex parte review could threaten national security if disclosed.[71] Such a special master would have a security clearance for highly sensitive information and would have extensive experience in intelligence.[72]

Conclusion

Protecting confidential attorney-client communications from interception and use by government defendants is a matter of fundamental fairness in civil litigation. Courts should give limited deference to government assertions of the state secrets privilege in civil cases where the plaintiffs suing the government can make a credible assertion that they have been subject to a

---

[65] *See Turkmen*, 2006 WL 4483151, at *3 (noting that after reviewing the defendants' in camera, ex parte submissions, the court "may require counsel for the defendants to make further arguments as to why the submissions (or designated parts of them) should remain under seal").

[66] Ellsberg v. Mitchell, 709 F.2d 51, 57 (D.C. Cir. 1983).

[67] *Hepting*, 439 F. Supp. 2d at 1010.

[68] *Al-Haramain Islamic Found.*, 451 F. Supp. 2d at 1229 (D. Or. 2006); *see also* Brian M. Tomney, Case Note, *Contemplating the Use of Classified or State Secret Information Obtained* Ex Parte *on the Merits in Civil Litigation:* Bl(a)ck Tea Society v. City of Boston, 57 Me. L. Rev. 641, 662 (2005) (suggesting that the government could "redact the material to a level that eliminates the underlying harm"); Note, *supra* note 42, at 587 (suggesting that courts order the information to be made "available in a restricted form that would satisfy security requirements").

[69] *See supra* Part II.

[70] *See Ellsberg*, 709 F.2d at 64 (stating that the court did not want to "discourage procedural innovation").

[71] *See* Fed. R. Evid. 706(a) ("The court may appoint any expert witnesses agreed upon by the parties, and may appoint expert witnesses of its own selection"); *Hepting*, 439 F. Supp. 2d at 1010 (proposing the appointment of an expert to assist the court in determining whether disclosure of any classified material about the program would create a "reasonable danger" of harming national security).

[72] *Id.* at 1010–11. The *Hepting* court also explained that this appointment would be the type of procedural innovation in state secrets determinations encouraged by the *Ellsberg* court.

warrantless surveillance program that could have captured confidential attorney-client communications. Through enhanced in camera, ex parte review combined with innovative procedural measures, courts could create a more appropriate balance between liberty and security when such surveillance threatens the confidentiality of attorney-client communications. These enhanced procedures are necessary to ensure that plaintiffs like Shakir Baloch are treated fairly and that our civil litigation system maintains its integrity.