Winter 2004

Protecting the Unpopular from the Unreasonable: Warrantless Monitoring of Attorney Client Communications in Federal Prisons

Teri D. Baxter, *University of Tennessee College of Law*

ARTICLES

PROTECTING THE UNPOPULAR FROM THE UNREASONABLE: WARRANTLESS MONITORING OF ATTORNEY CLIENT COMMUNICATIONS IN FEDERAL PRISONS

Teri Dobbins[+]

INTRODUCTION

Less than two months after the September 11, 2001 terrorist attack on New York and Washington, D.C.; Bureau of Prisons (BOP) regulation 28 C.F.R. § 501.3(d) was promulgated, allowing warrantless monitoring of communications between federal inmates and their attorneys.[1] Under this regulation, the Attorney General can order the Director of the Bureau of Prisons to monitor attorney-client communications based solely on the Attorney General's "reasonable suspicion" that a particular inmate "may use communications with attorneys or their agents to further or facilitate acts of terrorism."[2] The rule expressly applies to communications that fall within the attorney-client privilege.[3] Although the new rule caused an outcry from critics who denounced it as a violation of inmates' constitutional rights, the Attorney General defends the rule as necessary to protect the nation from further terrorist attacks.[4]

[+] Assistant Professor, Saint Louis University School of Law. B.A. Duke University, 1993; J.D. Duke University, 1997. The author thanks Professors Peter Marguiles, Sara Sun Beale, Robert Mosteller, Scott L. Silliman, Camille Nelson and Rodger Goldman for comments on drafts of this Article. The author also gratefully acknowledges the research assistance of Joshua Stegeman and Corey White.

1. The interim rule and request for comments were published at 66 Fed. Reg. 55,062 on October 31, 2001. The effective date of the rule was October 30, 2001, and the rule was codified at 28 U.S.C. § 501.3(d).

2. 28 C.F.R. § 501.3(d) (2003). The Attorney General may rely on information from the head of a federal law enforcement or intelligence agency. *Id.*

3. *Id.*

4. "[I]t is not the intention of this Justice Department to either [sic] disrupt the effective communication between lawyers and the accused, but it is neither our willingness to allow individuals to continue terrorist activities or other acts which would harm the American public by using their lawyers and those conversations to continue or extend acts of terrorism or violence against the American people." *Department of Justice Oversight: Preserving Our Freedoms While Defending Against Terrorism, Hearings Before the S. Comm. on the Judiciary*, 107th Cong. 329 (2001) (statement of Attorney General John Ashcroft) [hereinafter *DOJ Hearings*].

Much of the debate has focused on inmates' Sixth Amendment right to counsel,[5] and the erosion of the attorney-client privilege.[6] Less prominent in the debate is the question whether national security requires allowing the Attorney General to monitor communications between inmates and their counsel without first obtaining a warrant. In the years since the terrorist attacks of September 11, 2001, the government has taken numerous steps to increase national security and prevent future attacks.[7] Many Americans, desperate to regain a sense of security, have embraced—or at least tolerated—these efforts without pausing to consider the long-term effect on their civil liberties. Opposition is especially muted when the government targets the rights of suspected or convicted terrorists. However, not all possible measures have proven to be necessary or even prudent. Consequently, in addition to challenging the constitutionality of these measures, it has become necessary to challenge the government's implication that citizens must be willing to give the Executive greater authority in order to protect against terrorism while simultaneously freeing the Executive from traditional checks and balances that prevent any one branch of government from exercising unfettered power.

Another question that has received relatively little attention is whether warrantless monitoring violates inmates' rights under the Fourth Amendment to the United States Constitution?[8] Prior to enactment of 28 C.F.R. § 501.3(d) (monitoring regulation, or § 501.3(d)), federal and many state prison regulations forbade monitoring of inmate-attorney communications.[9] Consequently, the Supreme Court has not needed to decide whether monitoring without a warrant would violate the Fourth Amendment. Moreover, while a sound argument can be made that the right to confidential communications with attorneys is included in the Sixth Amendment right to counsel, that right does not extend to all persons within the scope of § 501.3(d).[10] The Fourth Amendment right to

---

5. U.S. CONST. amend VI.

6. *See, e.g., infra* note 46.

7. *See, e.g.*, Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act), Pub. L. No. 107-56, 115 Stat. 272 (Oct. 26, 2001) (including several amendments to the Foreign Intelligence Surveillance Act of 1978, 50 U.S.C.A. § 1801 *et seq.*, designed to give law enforcement officers greater authority to conduct searches and seizures).

8. U.S. CONST. amend IV.

9. *See infra* note 286.

10. The Sixth Amendment right to counsel does not attach until after the initiation of adversary judicial proceedings, whether by formal charge, indictment, information, or arraignment. Texas v. Cobb, 532 U.S. 162, 167 (2001). The monitoring regulation, on the other hand, applies to all inmates, defining "inmates" broadly to include all persons in the custody of the Federal Bureau of Prisons. 28 C.F.R. § 500.1(c).

private communications with attorneys applies to all federal inmates.[11] Finally, reliance on the Sixth Amendment alone is troublesome because of the conflicting precedent regarding Sixth Amendment privacy rights—courts disagree about whether the right is violated if the accused cannot prove that the monitoring of privleged communications prejudiced his or her right to a fair trial.[12] The uncertainty of the scope of Sixth Amendment privacy rights underscores the importance of exploring Fourth Amendment protections, in addition to those provided by the Sixth Amendment.

This Article considers whether § 501.3(d) is an unnecessary and unconstitutional exercise of Executive authority. While national security unquestionably is and should be one of the government's highest priorities, the Attorney General has the ability under existing statutes and rules, including the Omnibus Crime Control and Safe Streets Act of 1968, as amended (Title III),[13] the Foreign Intelligence Surveillance Act of 1978 (FISA),[14] and Federal Rule of Criminal Procedure 41,[15] to monitor attorney-client communications inside of prisons. Each of these statutes is more restrictive than § 501.3(d), but the restrictions, which include obtaining a warrant or order issued by a neutral magistrate or judge, are not unduly burdensome and serve the salient purpose of ensuring that the government does not abuse its power or arbitrarily deprive inmates of their rights.[16] This is especially important when the right at issue is as essential as the right to confidential attorney-client communications. Moreover, even national security concerns do not justify allowing the Executive, acting through the Attorney General, to bypass prior judicial review and act unilaterally in deciding when and

11. *See* U.S. CONST. amend IV; *see infra* Part IV.

12. *See generally* Martin R. Gardner, *The Sixth Amendment Right to Counsel and Its Underlying Values: Defining the Scope of Privacy Protection*, 90 J. CRIM. L. & CRIMINOLOGY 397 (2000) (reviewing Supreme Court and lower court opinions, documenting the substantial disagreement regarding the role of privacy protection under the Sixth Amendment, and urging judicial clarification of the function of attorney-client privacy in the right to counsel cases). Many articles and notes have been published that have ably addressed the question of whether the regulation violates inmates' Sixth Amendment rights. *See infra* note 45. This Article does not attempt to address the Sixth Amendment in depth. Instead, it simply points out that the Sixth Amendment alone may not provide a complete answer to the problem of protecting the confidentiality of attorney-client communications in federal prisons. At a minimum, considering whether the Fourth Amendment provides a right of privacy in addition to any rights under the Sixth Amendment is prudent.

13. 18 U.S.C. §§ 2510-2521 (2003).

14. 50 U.S.C. § 1801 (2003).

15. FED. R. CRIM. P. 41.

16. *See supra* notes 13-15.

under what circumstances attorney-client communications should be monitored.

In addition to being unnecessary, the rule violates inmates' Fourth Amendment right to privacy. While inmates' Fourth Amendment rights have been severely curtailed in many respects, their right to privacy has not been eliminated in all contexts. When society is prepared to recognize the right to privacy as reasonable, and exercise of the right does not interfere with prison administration or security, then the Fourth Amendment applies to protect inmates from unreasonable search or seizure. Traditionally, Americans have been prepared to recognize inmates' right to private communication with their attorneys as reasonable. Moreover, because § 501.3(d) is unnecessary to accomplish its stated goal of deterrence, and because there is no evidence requiring the Attorney General to seek a warrant before monitoring inmate-attorney communications that would jeopardize prison security or national security, the Fourth Amendment right to privacy should apply to inmate-attorney communications.

Finally, it is well settled that prison regulations that impinge on inmates' constitutional rights may be upheld only if they are rationally related to a legitimate penological objective. The monitoring regulation does not meet this test. It serves a general law enforcement objective, not a penological objective. Moreover, it leaves inmates without any other means of confidential communications with their lawyers. On the other hand, existing statutes give the government the authority to conduct monitoring, albeit with prior judicial approval and continuing oversight—both afford inmates a measure of protection against well-meaning but overzealous executive authorities—without imposing any undue burden on the government. Under these circumstances, the regulation is unreasonable, unconstitutional, and should be struck down.

Part I of this Article describes the legislative history of 28 C.F.R. § 501.3. It briefly discusses the controversy surrounding the 1997 rule and the October 31, 2001 amendment that added the monitoring regulation. Part II reviews provisions of Title III, FISA, and Federal Rule of Criminal Procedure 41, including their requirements for obtaining a warrant or order to intercept private communications such as attorney-client communications. Part III addresses the claim that national security concerns justify warrantless monitoring of inmates. It first examines the Executive's historic use of warrantless surveillance in the name of national security, and then reviews Supreme Court precedent holding that domestic threats to national security do not justify exempting the Executive from the Fourth Amendment warrant requirement. Next, Part III considers the Executive's more expansive power to conduct warrantless surveillance to gather foreign intelligence and the

curtailment of that power after enactment of FISA. The argument that warrantless monitoring of inmates is necessary to protect national security is then analyzed in light of Congress's and the Supreme Court's rejection of the same argument outside of the prison context.

Part IV discusses inmates' constitutional rights, and in particular, their Fourth Amendment rights. After establishing that inmates retain some Fourth Amendment protections, this Article asserts that inmates have a right to private communications with their attorneys that is protected by the Fourth Amendment. Finally, Part V reviews the legal standards for imposing restrictions on inmates' constitutional rights and applies those standards to the monitoring regulation, concluding that the rule violates inmates' Fourth Amendment right to privacy and must be struck down.

I. HISTORY OF 28 C.F.R. § 501.3(d)

Entitled "Prevention of Acts of Violence and Terrorism," 28 C.F.R. § 501.3 was promulgated in 1997, amending the existing § 501.[17] The interim rule and request for comments were published on May 17, 1996, and the rule was finalized and took effect on June 20, 1997.[18] Like the 2001 amendment, the original § 501.3 was designed to protect the public from acts of terrorism.[19] The rule allows the Bureau of Prison (BOP) Director to authorize the warden to implement special administrative measures upon written notice "that there is a substantial risk that a prisoner's communications or contacts with persons could result in death or serious bodily injury to persons, or substantial damage to property that would entail the risk of death or serious bodily injury to persons."[20]

The precise measures to be implemented are left to the warden's discretion; the regulation simply authorizes the warden to implement "reasonably necessary" measures.[21] Measures suggested in the regulation include housing the inmate in administrative detention and limiting certain privileges such as correspondence, visiting, interviews with the

17. 62 Fed. Reg. 33,730 (June 20, 1997) (codified at 28 C.F.R. pt. 501). Title 28 of the Code of Federal Regulations deals with Judicial Administration. *Id.* at 33,732. Section 501.3 is in Part IV Department of Justice, Bureau of Prisons, Subchapter A—General Management and Administration, Part 501—Scope of Rules.

18. *Id.*

19. The Supplementary Information published with the interim rule and request for comments stated that the BOP "is adopting interim regulations on the correctional management of inmates whose contacts with other persons present the potential for acts of violence and terrorism. Under these interim regulations, the Warden may implement administrative measures that are reasonably necessary to protect the public against such acts." 61 Fed. Reg. 25,120.

20. 62 Fed. Reg. at 33,732.

21. *Id.*

news media, and use of the telephone.[22] The prison staff is required to provide the affected inmate with written notification that restrictions have been imposed and the basis for the restrictions, although the basis for the restrictions can be limited "in the interest of prison security or safety or to protect against acts of violence or terrorism."[23]

The BOP received numerous comments in response to the publication of the interim rule. The majority of the comments concerned the First Amendment implications of the regulation.[24] Indeed, the majority of the BOP's response to the comments, published with the final rule on June 20, 1997, addressed the First Amendment issue and argued that the rule was consistent with Supreme Court standards for restrictions on freedom of speech and freedom of the press.[25] The BOP noted that, while the Supreme Court in *Pell v. Procunier* held that prison inmates retain those First Amendment rights that are consistent with their status as inmates and "with the legitimate penological objectives of the corrections system," deterrence of crime is an important function of the corrections system and "central to all other corrections goals" is internal prison security.[26] The BOP asserted its belief that § 501.3 is consistent with those objectives and permissible under Supreme Court precedent.[27]

The BOP's response indicated that at least one comment questioned the necessity of the rule, but was apparently based on the fact that no

---

22. *Id.*

23. *Id.*

24. *Id.* at 33,730

25. *Id.* The BOP's published response to the comments acknowledged that:

> Comments generally expressed concern that the regulation is violative of a person's First Amendment rights, with one commenter stating that the First Amendment "prohibits governmental interference with freedom of speech and freedom of press."
>
> . . . .
>
> Other commenters acknowledge that the regulation was promulgated in order to protect the safety of government officials and the general public . . . . Notwithstanding this acknowledgment, these commenters also addressed the First Amendment issue . . . . Other comments said that the regulation may prevent the press from fully reporting on the very people who "may threaten society the most", [sic] and that the regulation forecloses other avenues of obtaining information; that the "complete ban suggested by the regulation * * * is legally impermissible' [sic]; and that the regulation is imposed "without sufficient checks and balances to challenge government action."

Id. The response acknowledged still other commenters who expressed concern that the regulation was overbroad and indiscriminately barred the expression of speech that did not pose a threat to Federal officials or those outside of prison. *Id.* At least one commenter criticized the lack of a formal administrative measure by which non-inmates could challenge the restrictions as applied to a particular inmate. *Id.*

26. *Id.*

27. *Id.*

such rule had existed in the past and the commenter believed that "no death or injury ha[d] resulted" from communications between a federal inmate and someone outside of prison.[28] The BOP disagreed with the suggestion that death or injury must occur before preventive regulations could be implemented.[29] Despite the criticisms voiced in the comments, the rule was implemented and remains in force.[30]

On October 31, 2001, the Attorney General published an interim rule and request for comments regarding amendments to § 501.[31] One of the amendments was the addition of § 501.3(d), the monitoring regulation.[32] The 1997 rule did not specifically mention attorney-client communications, but the government acknowledged that attorney-client communications were not subject to monitoring under the existing regulations.[33] Section 501.3(d) authorizes the Attorney General to order the Director of the BOP to monitor or review communications between inmates and their attorneys or their attorneys' agents if "reasonable suspicion exists to believe that a particular inmate may use communications with attorneys or their agents to further or facilitate acts of terrorism."[34] According to the text of the rule, the purpose of

---

28. *Id.*

29. *Id.*

30. *See* Prevention of Acts of Violence and Terrorism, 28 C.F.R. § 501.3 (2003). The rule was amended in 2001, when subsection (d) was added, but the changes were not in response to earlier criticisms; indeed, the amendments expanded the Attorney General's authority. *Id.*

31. National Security; Prevention of Acts of Violence and Terrorism, 66 Fed. Reg. 55,062 (Oct. 31, 2001). Although it was dubbed an interim rule, the effective date of the rule was the day before the interim rule was published in the Federal Register. *Id.* No final rule or response to comments was published in the Federal Register.

32. *Id.* at 55,063-64.

33. *Id.* The interim rule noted, "[i]n general, the Bureau's existing regulations relating to special mail (§§ 540.18, 540.19), visits (§ 540.48), and telephone calls (§ 540.103) contemplate that communications between an inmate and his or her attorney are not subject to the usual rules for monitoring of inmate communications." *Id.*

34. 28 C.F.R. § 501.3(d). The rule reads:

> In any case where the Attorney General specifically so orders, based on information from the head of a federal law enforcement or intelligence agency that reasonable suspicion exists to believe that a particular inmate may use communications with attorneys or their agents to further or facilitate acts of terrorism, the Director, Bureau of Prisons, shall, in addition to the special administrative measures imposed under paragraph (a) of this section, provide appropriate procedures for the monitoring or review of communications between that inmate and attorneys or attorneys' agents who are traditionally covered by the attorney-client privilege, for the purpose of deterring future acts that could result in death or serious bodily injury to persons, or substantial damage to property that would entail the risk of death or serious bodily injury to persons.
> (1) The certification by the Attorney General under this paragraph (d) shall be in addition to any findings or determinations relating to the need for the

monitoring is not to gather evidence of past crimes, but to deter inmates from committing future acts that could result in death or serious bodily injury.[35] "Inmate" is defined broadly to include "all persons in the custody of the Federal Bureau of Prisons or Bureau contract facilities."[36] This category includes not only persons charged with or convicted of criminal offenses, but also persons held as "witnesses, detainees, or otherwise."[37] Thus, some of the persons subject to monitoring may not even be suspected or accused of criminal activity.

The Attorney General claims that the regulation "recognize[s] the existence of the attorney-client privilege and an inmate's right to counsel," and that the safeguards included in the rule protect those rights.[38] Specifically, the monitoring regulation requires the Director to employ "appropriate procedures" for reviewing the communications for privilege claims and to ensure that "properly privileged materials" are

---

imposition of other special administrative measures as provided in paragraph (a) of this section, but may be incorporated into the same document.

(2) Except in the case of prior court authorization, the Director, Bureau of Prisons, shall provide written notice to the inmate and to the attorneys involved, prior to the initiation of any monitoring or review under this paragraph (d). The notice shall explain:

(i) That, notwithstanding the provisions of part 540 of this chapter or other rules, all communications between the inmate and attorneys may be monitored, to the extent determined to be reasonably necessary for the purpose of deterring future acts of violence or terrorism;

(ii) That communications between the inmate and attorneys or their agents are not protected by the attorney-client privilege if they would facilitate criminal acts or a conspiracy to commit criminal acts, or if those communications are not related to the seeking or providing of legal advice.

(3) The Director, Bureau of Prisons, with the approval of the Assistant Attorney General for the Criminal Division, shall employ appropriate procedures to ensure that all attorney-client communications are reviewed for privilege claims and that any properly privileged materials (including, but not limited to, recordings of privileged communications) are not retained during the course of the monitoring. To protect the attorney-client privilege and to ensure that the investigation is not compromised by exposure to privileged material relating to the investigation or to defense strategy, a privilege team shall be designated, consisting of individuals not involved in the underlying investigation. The monitoring shall be conducted pursuant to procedures designed to minimize the intrusion into privileged material or conversations. Except in cases where the person in charge of the privilege team determines that acts of violence or terrorism are imminent, the privilege team shall not disclose any information unless and until such disclosure has been approved by a federal judge.

35. 28 C.F.R. § 501.3(d).

36. § 500.1(c).

37. *Id.*

38. National Security, Prevention of Acts of Violence and Terrorism, 66 Fed. Reg. at 55,064.

not retained.[39] Additionally, to protect the attorney-client privilege and to avoid compromising the underlying prosecution, a "privilege team" consisting of individuals unassociated with the underlying investigation will be designated to ensure that privileged material is not disclosed to the prosecution team.[40] Unless the head of the privilege team determines that acts of violence or terrorism are imminent, no information gathered from monitoring may be disclosed to anyone without approval from a federal judge.[41]

Finally, the government monitoring is not covert. Unless prior court authorization has been obtained, the Director must provide written notification to the inmate and the attorneys involved before monitoring begins.[42] While the inmate and attorney have notice of the monitoring, the regulation does not provide any mechanism for challenging the determination that an inmate qualifies for monitoring under the standard set out in the regulation, nor does it provide for any judicial oversight of the monitoring or the procedures for protecting the attorney-client privilege.[43]

Many prominent legal, law enforcement, human rights, civil liberty, and religious scholars and organizations submitted comments criticizing the new rule, arguing that it violates inmates' First, Fourth, Fifth, Sixth, and Fourteenth Amendment rights.[44] Much of the analysis in subsequent

---

39. § 501.3(d)(3).

40. *Id.* The Interim Rule reads:

> In following these procedures, it is intended that the use of a taint team and the building of a firewall will ensure that the communications which fit under the protection of the attorney-client privilege will never be revealed to prosecutors and investigators. Procedures such as this have been approved in matters such as searches of law offices . . . . In a similar vein, screening procedures are used in wiretap surveillance.

National Security, Prevention of Acts of Violence and Terrorism, 66 Fed. Reg. at 55,064 (citing *National City Trading Corp. v. United States*, 635 F.2d 1020, 1026-27 (2d Cir. 1980) and *United States v. Noriega*, 764 F. Supp. 1480 (S.D. Fla. 1991)).

41. § 501.3(d)(3).

42. § 501.3(d)(2).

43. *See generally* § 501.3.

44. *See, e.g.*, Comments from the American Bar Association submitted December 28, 2001 (on file with author); Joint comments from the American Civil Liberties Union, American Immigration Lawyers Association, Arab American Institute, Asian American Legal Defense Education Fund, Center for Democracy & Technology, DV Prisoners' Legal Services Project, Electronic Privacy Information Center, Equal Justice Program, Howard University School of Law, Friends Committee on National Legislation, Lawyers Committee for Human Rights, Legal Action Center, Legal Aid Society of New York, Libertarian Party, The Multiracial Activist, National Association for the Advancement of Colored People, National Black Police Association, Unitarian Universalist Association of Congregations, Washington Council of Lawyers, and World Organization Against Torture, submitted December 20, 2001 (on file with author).

comments, notes, and articles has focused on inmates' Sixth Amendment right to counsel, implications for the attorney-client privilege, and the chilling effect the rule may have on communications between inmates and their attorneys.[45] Government officials defend the regulation as a valid and constitutional exercise of Executive authority that is necessary to ensure national security.[46] However, the government's arguments in support of the regulation only address Supreme Court precedent regarding the Sixth Amendment rights of inmates.[47] Thus, the presumption that the regulation is constitutional fails to consider whether inmates' Fourth Amendment rights are violated. The government also fails to acknowledge precedent restricting the executive's authority to conduct warrantless searches, even in cases of threats to national security.[48]

---

45. *See, e.g.*, Marjorie Cohn, *The Evisceration of the Attorney-Client Privilege In the Wake of September 11, 2001*, 71 FORDHAM L. REV. 1233, 1234 (2003) (analyzing "the attack on the attorney client privilege since September 11, 2001 [and] warn[ing] of the dangers that undermining the attorney-client privilege poses to the United States criminal justice system"); Avidan Y. Cover, *A Rule Unfit for All Seasons: Monitoring Attorney-Client Communications Violates Privilege and the Sixth Amendment*, 87 CORNELL L. REV. 1233, 1234-35 (2002); Peter Margulies, *The Virtues and Vices of Solidarity: Regulating the Roles of Lawyers for Clients Accused of Terrorist Activity*, 62 MD. L. REV. 173, 190-91 (2003) (discussing the effect of monitoring on the attorney-client relationship); Ronald D. Rotunda, *Monitoring the Conversations of Prisoners*, 13 No. 3 PROF. LAW. 1, 10 (Spring 2002) (analyzing the new regulation in light of Sixth Amendment precedent and concluding that existing law "seems to be on the side of rejecting a per se prohibition against monitoring in this kind of situation").

46. National Security; Prevention of Acts of Violence and Terrorism, 66 Fed. Reg. at 55,062-64. In comments published with the interim rule, the government cited *Weatherford v. Bursey*, 429 U.S. 545 (1977), in support of its contention that no Sixth Amendment violation occurs when attorney-client conversations are monitored so long as privileged communications are protected from disclosure and no information recovered through monitoring is used by the government in a way that impairs an inmate's right to a fair trial. National Security; Prevention of Acts of Violence and Terrorism, 66 Fed. Reg. at 55,064. The government further stated that the "rule carefully and conscientiously balances an inmate's right to effective assistance of counsel against the government's responsibility to thwart future acts of violence or terrorism perpetrated with the participation or direction of federal inmates." *Id.*; *see also* Viet D. Dinh, *Freedom and Security After September 11*, 25 HARV. J. L. & PUB. POL'Y 399, 404 (2002) (describing the new regulation as merely closing a loophole left open by prior regulations and arguing that it adequately protects the attorney-client privilege); *Administration Defends Military Commissions, Other Antiterrorism Measures During Senate Hearing*, 78 No. 46 Interpreter Releases 1809-10 (December 3, 2001) (citing testimony of Senator Orrin G. Hatch (R-Utah) stating that the regulation is consistent with Supreme Court precedent regarding monitoring of attorney-client communications, and citing the testimony of Assistant Attorney General Michael Chertoff, stating that the regulation merely extended pre-existing special administrative measures to permit the monitoring of the attorney-client communications of a very small group of inmates).

47. *See id.*

48. *See infra* Part III.

II. FEDERAL STATUTES AND RULES ALLOWING MONITORING OR SEIZURE OF ATTORNEY-CLIENT COMMUNICATIONS

Section 501.3(d) does not specify how to conduct the monitoring. Presumably, communications between inmates and their attorneys could be monitored using electronic surveillance of oral or telephone communications, having monitors physically present listening to the communications, or by reviewing mail to and from attorneys. It is undisputed that except in a few limited circumstances, all of these types of monitoring require authorities to first obtain a warrant outside of the prison context.[49] The same should hold true for monitoring inside of prisons.

Title III is the federal statute that regulates interception of wire, oral, and electronic communications in general, and it sets out the required procedures when obtaining a warrant for such interceptions.[50] Federal Rule of Criminal Procedure 41 outlines the procedure for seizing property such as letters, books, or papers. If the target is an agent of a foreign power,[51] surveillance operates in accordance with the Foreign Intelligence Surveillance Act.

A. Title III

Title III "represents a comprehensive attempt by Congress to promote more effective control of crime while protecting the privacy of individual thought and expression."[52] Much of the Act was designed to meet the constitutional requirements for electronic surveillance enumerated by the United States Supreme Court in *Berger v. New York*[53] and *Katz v. United States*;[54] both were decided the year before Title III was enacted.[55]

---

49. *See* 18 U.S.C. § 2511 (2001)(requiring a court order or other written notification for law enforcement to obtain intercepted or disclosed wire, oral, or electronic communications from service providers); FED. R. CRIM. P. 41 (discussing the search and seizure warrant requirement); Berger v. New York, 388 U.S. 41, 48-49 (1967) (noting federal law on official wiretap interception); Katz v. United States, 389 U.S. 347, 358-59 (1967) (discussing the Fourth Amendment right against unreasonable searches and seizures).

50. 18 U.S.C. § 2510-2522 (2003).

51. 50 U.S.C. § 1801 (2003) (defining "agent of a foreign power"). *See infra* Part II.C.

52. United States v. United States Dist. Ct. *(Keith)*, 407 U.S. 297, 302 (1972). Title III regulates both law enforcement and private conduct. Bartnicki v. Vopper, 532 U.S. 514, 523 (2001).

53. 388 U.S. 41 (1967).

54. 380 U.S. 347 (1967).

55. *Bartnicki*, 532 U.S. at 522-23 (discussing background of Title III and citing Berger v. New York, 388 U.S. 41 (1967), and Katz v. United States, 389 U.S. 347 (1967)).

In *Berger v. New York,* the Supreme Court held that New York's wiretap statute violated the Fourth Amendment.[56] The Court held that the statute satisfied the Fourth Amendment requirement that a neutral and detached authority issue the order, but it failed to require a particular description of the crime committed or about to be committed, or a specific description of the persons or things to be searched or seized.[57] Furthermore, the length of the authorization was determined to be too long, and the statute placed no termination date on the eavesdrop once the conversation was seized.[58] Finally, the statute neither required notice to the search or surveillance target, nor a showing of special or exigent circumstances to avoid the notice requirement.[59] The Court concluded, "In short, the statute's blanket grant of permission to eavesdrop is without adequate judicial supervision or protective procedures."[60]

A few months later, the Supreme Court decided *Katz v. United States.*[61] Mr. Katz was convicted of transmitting wagering information from Los Angeles to Miami and Boston in violation of federal law.[62] Evidence used against him at trial included his end of telephone conversations that took place in a public phone booth.[63] FBI agents listened to and recorded the conversations using listening devices they had attached to the outside of the phone booth.[64] No warrant had been obtained to authorize the surveillance.[65] The Government successfully argued to the trial court and the court of appeals that no warrant was necessary because there was no physical intrusion into the area occupied by Mr. Katz.[66]

The Supreme Court disagreed, noting:

> [T]he Fourth Amendment protects people, not places. What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection . . . But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.[67]

---

56. *Berger*, 388 U.S. at 62-63.
57. *Id.* at 54, 56.
58. *Id.* at 59.
59. *Id.* at 60.
60. *Id.*
61. 389 U.S. 347 (1967).
62. *Id.* at 348.
63. *Id.*
64. *Id.*
65. *Id.* at 348, 356-57.
66. *Id.* at 348-49.
67. *Id.* at 351, 352.

The question, then, was whether the search complied with Fourth Amendment standards.[68] The government claimed that while the search was conducted without a warrant, the search was reasonable and conducted under circumstances in which a magistrate might properly have issued a warrant, had one been sought.[69] The Court declined to sanction the search on that basis, emphasizing that "[s]earches conducted without warrants have been held unlawful 'notwithstanding facts unquestionably showing probable cause.'"[70] Because the agents failed to comply with the requirements of the Fourth Amendment before conducting the surveillance, and because the surveillance led to Mr. Katz's conviction, the judgment was reversed.[71]

Congress enacted Title III the year following the *Berger* and *Katz* decisions. It was designed to balance the needs of law enforcement with the requirements of the Fourth Amendment, outlined by the Supreme Court in those cases. Section 2516 of the Act provides authorization to intercept wire, oral, and electronic communications and states that the Attorney General may authorize an application to a federal judge for an order authorizing or approving the interception of communications by the FBI or other federal agencies when the interception may provide evidence of terrorist activities.[72] The application must fully and completely state the facts and circumstances justifying the applicant's belief "that an order should be issued,"[73] state the time period for which

68. *Id.* at 354.

69. *Id.*

70. *Id.* at 356-57 (quoting Agnello v. United States, 269 U.S. 20, 33 (1925)).

71. *Id.* at 359.

72. 18 U.S.C. § 2516(1)(q), (r) (2000 & Supp. 2003). The Deputy Attorney General, Associate Attorney General, any Assistant Attorney General, any acting Assistant Attorney General, or any Deputy Assistant Attorney General or acting Deputy Assistant Attorney General in the Criminal Division specially designated by the Attorney General has the same authority to authorize applications for orders authorizing interception of wire or oral communications. § 2516(a)(1). The judge may also grant orders authorizing interception of communications that may provide evidence of numerous other offenses under title 18, including: Presidential and Presidential staff assassination, kidnapping, and assault (§ 1751); hostage taking (§ 1203); destruction of aircraft or aircraft facilities (§ 32); threatening or retaliating against a federal official (§ 115); congressional, Cabinet, or Supreme Court assassinations, kidnapping, and assault (§ 351); wrecking trains (§ 1992); production of false identification documents (§ 1028); and fraud and misuse of visas, permits, and other documents (§ 1546)). § 2516(1)(c), (p). Likewise, orders may be issued to obtain evidence of violations of section 274, 277, or 278 of the Immigration and Nationality Act, which relate to alien smuggling. § 2516(1)(p).

73. § 2518(1)(b). The statement should include details about the offense that is being or about to be committed, a description of the nature and location of the place where the communication is to be intercepted, a description of the type of communications to be intercepted, and "the identity of the person, if known, committing the offense and whose communications are to be intercepted." *Id.* It must also state whether "other investigative

the interception will be maintained,[74] and disclose facts concerning all previous applications known to the applicant and any action taken on such applications.[75] The judge may require additional evidence to support the application.[76]

The judge may approve the application and issue an *ex parte* order authorizing the interception if the judge determines that:[77] (a) there is probable cause to believe that an individual is committing, has committed, or is about to commit one of the offenses covered by the Act;[78] (b) there is probable cause to believe that communications concerning that offense will be obtained through the interception;[79] (c) "normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous";[80] (d) with limited exceptions,[81] probable cause exists to believe "that the facilities from which, or the place where, the wire, oral, or electronic communications are to be intercepted are being used, or are about to be used, in connection with the commission of such offense, or are leased to, listed in the name of, or commonly used" by the surveillance target.[82]

Title III also includes a provision authorizing warrantless surveillance in the event of an emergency.[83] However, an application for authorization must be made within forty-eight hours of the time an interception has occurred or begins to occur.[84] The interception must terminate immediately once the application is denied or the targeted interception is obtained, whichever occurs first.[85]

---

procedures have been tried and failed, or why [such procedures] reasonably appear to be unlikely to succeed if tried or [why such procedures would] be too dangerous." § 2518(1)(c).

74. § 2518(1)(d).

75. § 2518(1)(e).

76. § 2518(2).

77. *See* § 2516(1), (2).

78. § 2518(3)(a).

79. § 2518(3)(b).

80. § 2518(3)(c).

81. *See* § 2518(11).

82. § 2518(3)(d).

83. § 2518(7). An emergency situation exists if it involves "(i) immediate danger of death or serious physical injury to any person, (ii) conspiratorial activities threatening the national security interest, or (iii) conspiratorial activities characteristic of organized crime." *Id.*

84. *Id.*

85. *Id.* If the application is denied, or the "interception is terminated without an order having been issued, the contents of any wire, oral, or electronic communication intercepted shall be treated as having been obtained in violation of [Title III]." § 2518(7)(b).

When it was originally enacted, Title III included a provision stating that the Act was not intended to limit the President's constitutional power to conduct foreign intelligence surveillance or to protect national security.[86] This provision, § 2511(3), was deleted in 1978 and § 2511 was amended to expressly state Congress' intent that Title III be the exclusive means for conducting electronic surveillance.[87] Section 2511 now states that except as permitted under Title III, any person who intercepts or attempts to intercept wire, oral, or electronic communications is subject to punishment, including imposition of a fine, imprisonment for up to five years, or both.[88]

Although it is agreed that Title III applies to prison monitoring in general,[89] the routine monitoring of communications with non-attorneys has been held to fall within one or both of two exceptions to Title III.[90]

---

86. *See* § 2511 (2000) (Amendments); *see also* United States v. United States Dist. Court (Keith), 407 U.S. 297, 303 (1972) (analyzing the effect of this provision on the President's authority to conduct warrantless searches in the name of national security).

87. *See* § 2511 (2000) (Amendments). Foreign intelligence surveillance, which is governed by other federal laws, including FISA, is excepted from this statute. § 2511(f).

88. § 2511(1), (4). "Person" is defined as "any employee, or agent of the United States or any State or political subdivision thereof, and any individual, partnership, association, joint stock company, trust, or corporation." § 2510(6).

89. *See, e.g.*, United States v. Amen, 831 F.2d 373, 378 (2d Cir. 1987) (stating that "Title III clearly applies to prison monitoring."). An argument could be made that Title III does not apply to oral communications in prison because inmates have no justifiable expectation of privacy in those communications. Wire communication (which include telephone conversations) is defined in Title III to include "any aural transfer" made using wire, cable, or other similar equipment. § 2510(1). The definition makes no reference to the speaker's expectation of privacy. Consequently, all wire communication is subject to Title III, regardless of the speaker's expectation of privacy. *See* John Ashcroft, Memorandum for the Heads and Inspectors General of Executive Departments and Agencies: Procedures for Lawful, Warrantless Monitoring of Verbal Communications, May 2002 (on file with author) ("As a general rule, nonconsensual interceptions of wire communications violate 18 U.S.C. § 2511 regardless of the communicating parties' expectation of privacy, unless the interceptor complies with the court-authorization procedures of Title III . . . or with the provisions of the Foreign Intelligence Surveillance Act of 1978 . . . ."). Oral communication, on the other hand, "means any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception *under circumstances justifying such expectation.*" § 2510(2) (emphasis added). Thus, if no justifiable expectation of privacy exists in an oral communication, Title III does not cover the communication. It could be argued that inmates have no justifiable expectation of privacy in their oral communications in prison generally, but as demonstrated below, inmates have a justifiable expectation of privacy when communicating with their attorneys while incarcerated. Those communications, then, are covered by Title III. *See infra* Part IV.C.

90. Several inmates have also challenged monitoring of non-privileged telephone calls from prisons on Fourth Amendment grounds. *See, e.g.*, United States v. Van Poyck, 77 F.3d 285, 291 (9th Cir. 1996); *Amen*, 831 F.2d at 379-80. Most courts have rejected such challenges on the grounds that inmates have no reasonable expectation of privacy in their calls from prison that would trigger Fourth Amendment protection, and even if the Fourth

First, under § 2511(c), Title III is not violated if a person acting under color of law intercepts a communication when one of the parties to the communication has consented to the interception.[91] The legislative history confirms that Congress intended for the consent to include express and implied consent.[92] For example, apartment residents and bank customers are deemed to impliedly consent to the use of security devices in apartment buildings or in banks.[93] In the prison context, courts have held that inmates impliedly consent to recording and monitoring of telephone calls—except to attorneys—particularly when inmates are informed before placing calls that their conversations will be monitored.[94]

Courts have also held that prison monitoring falls within the law enforcement exception to Title III. While § 2811 of the Act generally prohibits use of any electronic, mechanical, or other device to intercept communications, § 2510(5)(a)(ii) states that "electronic, mechanical, or other device" does not include any device or apparatus that is being used "by an investigative or law enforcement officer in the ordinary course of his duties."[95] Several circuits have held that when law enforcement officials use devices to record or monitor all non-privleged inmate telephone calls, this use falls within the ordinary course of their duties.[96] In cases where this exception has been applied, the inmates had notice that the calls were subject to recording or monitoring. At least one court has required such notice for the exception to apply.[97]

Amendment were triggered, institutional security concerns renders such monitoring reasonable for Fourth Amendment purposes. *Van Poyck*, 77 F.3d at 291; *Amen*, 831 F.2d at 379-80.

91. § 2511(2)(c).

92. S. REP. NO. 90-1097 (1968).

93. *Amen*, 831 F.2d at 378 (quoting S. REP. NO. 90-1097 (1968), *reprinted in* 1968 U.S.C.C.A.N. 2112, 2182).

94. *See Van Poyck*, 77 F.3d at 292 (holding that consent exception to Title III applied when signs were posted above telephones that warned that phone calls were subject to monitoring and taping, when the inmate signed a form consenting to monitoring, and when the inmate received a prison manual outlining monitoring procedures); *Amen*, 831 F.2d at 379. *See also* United States v. Gangi, 57 Fed. Appx. 809, 813 (10th Cir. 2003). In *Gangi*, the court held that the inmate impliedly consented to the taping of his phone calls even though there were no signs posted above the specific phone that he used informing him that calls would be recorded. *Id.* at 813. Instead, the court found that notices placed above the phones in other areas of the prison, in which the inmate had spent significant time, were sufficient to place him on notice that any calls he made—except calls on specific phones to attorneys—would be recorded. *Id.* at 813-14.

95. § 2510(5)(a)(ii).

96. *Van Poyck*, 77 F.3d at 292; United States v. Feekes, 879 F.2d 1562, 1565-66 (7th Cir. 1989); United States v. Paul, 614 F.2d 115, 117 (6th Cir. 1980), *cert. denied*, 446 U.S. 941 (1980).

97. Adams v. City of Battle Creek, 250 F.3d 980, 984 (6th Cir. 2001). The court held:

Neither of these exceptions, nor any others under Title III, have been applied to monitoring of communications between inmates and their attorneys. Such monitoring never has been conducted in the ordinary course of law enforcement officers' duties and never has consent to monitoring of attorney-client communications been implied as it has in the case of communication with non-attorneys.[98] While nothing in Title III expressly distinguishes between these two classes of communications, courts and prison administrators had almost uniformly protected and respected the confidentiality of attorney-client communications before § 501.3(d) was enacted.[99] The Attorney General even acknowledged that prior BOP regulations did not authorize monitoring of communications with attorneys.[100]

B. Federal Rule of Criminal Procedure 41

Title III does not authorize physical searches. However, federal law enforcement officers can obtain a warrant to seize tangible items such as letters, books, or other papers under Federal Rule of Criminal Procedure 41.[101] The warrant may be issued for evidence of a crime (including domestic or international terrorism), contraband, fruits of a crime, items in possession illegally, and property intended for use or used in committing a crime.[102] The warrant must be issued by the magistrate or state court judge if, after reviewing an affidavit or other information from a federal law enforcement officer or attorney for the government, probable cause exists to search for and seize any of this type of

---

> There is some disagreement in the case law about whether "covert" monitoring can ever be in the "ordinary course of business." Although we do not find that the statute requires actual consent for the exception to apply, we do hold that monitoring in the ordinary course of business requires notice to the person or persons being monitored.

Id.

98. In most cases, prisons have specific phones for calls to attorneys and inmates are informed that conversations on these phones will not be monitored. Consequently, it would be difficult to construct a convincing argument that inmates have consented to monitoring of conversations with their attorneys if they use one of these designated phones. *See, e.g.*, Monitoring of Inmate Telephone Calls, 28 C.F.R. § 540.102 (2002) ("Staff may not monitor an inmate's properly placed call to an attorney. The Warden shall notify an inmate of the proper procedures to have an unmonitored telephone conversation with an attorney.").

99. *See, e.g.*, Small v. Superior Court, 79 Cal. App. 4th 1000, 1010 (Cal. Dist. Ct. App. 2000) (noting that it is "indisputable that [inmates] ha[ve] the right to effective assistance of counsel, which includes the right to confer with counsel in absolute privacy."); 28 C.F.R. §§ 540.18, 540.102, 543.13 (exempting telephone, mail, and oral communications with attorneys from monitoring in federal prisons).

100. *See* 66 Fed. Reg. 55,062, 55,063.

101. FED. R. CRIM. P. 41(a)(2)(A).

102. FED. R. CRIM. P. 41(c).

property.[103] The executing officer must give a copy of the warrant and a receipt for the property seized to the person from whom it is taken, or leave a copy of the warrant and receipt at the place from which the property was taken.[104]

Prior to passage of the Patriot Act, some courts approved of magistrates issuing warrants that allowed officers to covertly inspect or photograph, but not physically seize, property.[105] Under these so-called "sneak and peek" warrants, notice that the warrant had been issued and executed could be delayed when law enforcement deemed nondisclosure of the search to be essential to the investigation.[106] Covert-entry warrants only could be issued if officers made a showing of reasonable necessity for the delay, and the delay only could be authorized for a reasonable time.[107] It was unclear whether this practice was authorized under FED. R. CRIM. P. 41.[108]

Section 213 of the Patriot Act clarified the authority of the courts. Under this section, a judge or magistrate who issues a warrant, under any law, to search for *but not seize* evidence of a crime, may authorize a delay in giving the required notice that the warrant has been executed if the court has reasonable cause to believe that immediate notification will have an "adverse result."[109] The warrant must provide for notice within a reasonable time; however, the court may grant extensions for good cause.[110]

---

103. FED. R. CRIM. P. 41(d)(1). The judge may require an affiant to appear personally to testify under oath. FED. R. CRIM. P. 41(d)(2)(A).

104. FED. R. CRIM. P. 41(e)(2),(f)(3).

105. *See* United States v. Villegas, 899 F.2d 1324, 1336-37 (2d Cir. 1990).

106. United States v. Heatley, No. 511 96 CR.515 (SS), 1998 WL 691201, at *2 (S.D.N.Y. Sept. 30, 1998) (citing United States v. Villegas, 899 F.2d at 1336-38).

107. *Id.* at *3. Extensions could be granted for good cause provided that each extension was based on a fresh showing of the need for the delay. *Id.* at *2-3 (quoting *Villegas*, 899 F.2d at 1337).

108. ACLU v. United States Dep't of Justice, 265 F.2d 20, 24 (D.C. Cir. 2003) (noting that before the Patriot Act, a court's ability to approve sneak and peek warrants was not entirely settled).

109. USA PATRIOT Act § 213, 18 U.S.C. § 3103a(b) (2002). "Adverse result" is defined as "(A) endangering the life or physical safety of an individual; (B) flight from prosecution; (C) destruction of or tampering with evidence; (D) intimidation of potential witnesses; or (E) otherwise seriously jeopardizing an investigation or unduly delaying a trial." § 2705(a)(2). Delayed notification is generally only allowed if the warrant prohibits seizure of tangible property. § 3103a(b). Under § 3103a(b)(2), however, seizure may be permitted if the court finds it a "reasonable necessity." *Id.*

110. 18 U.S.C. § 3103a(b)(3) (Supp. 2003). This provision of the Patriot Act has been criticized and Rep. Otter (R-ID) has introduced a bill to amend it. See H.R. 3352, 108th Cong. (1st Sess. 2003). The amended statute deletes the "adverse result" language and instead would only allow delayed notice "if the court finds reasonable cause to believe that providing immediate notification of the execution of the warrant will endanger the life or

C. Foreign Intelligence Surveillance Act of 1978 (FISA)

FISA was enacted to resolve disagreements in the courts of appeals regarding whether the President had inherent power to conduct warrantless surveillance to gather foreign intelligence information in the interest of national security.[111] One court noted that "FISA thus created a 'secure framework by which the Executive Branch may conduct legitimate electronic surveillance for foreign intelligence purposes within the context of this Nation's commitment to privacy and individual rights.'"[112] While the Attorney General is authorized to conduct warrantless searches in limited circumstances,[113] much of the foreign intelligence surveillance implicated by § 501.3(d) would likely require an order under FISA.[114]

---

physical safety of an individual, result in flight from prosecution, or result in the destruction of or tampering with the evidence sought under the warrant. *Id.* Additionally, instead of allowing delay for a "reasonable time," notice must be given within "seven calendar days," with extensions for additional seven calendar day periods if the court finds "reasonable cause to believe that notice of the execution of the warrant will endanger the life or physical safety or an individual, result in flight from prosecution, or result in the destruction of or tampering with the evidence sought under the warrant." *Id.*

111. ACLU Found. of S. Cal. v. Barr, 952 F.2d 457, 460-61 (D.C. Cir. 1991). FISA did not completely resolve this debate, and some courts, including the FISA Court of Review, believe that the President still has inherent authority to conduct foreign intelligence surveillance, although the scope of that authority has not been defined by the Supreme Court. *See In re* Sealed Case, 310 F.3d 717, 742 (Foreign Int. Surv. Ct. Rev. 2002). FISA has, however, significantly muted the debate.

112. *ACLU Found. of S. Cal.*, 952 F.2d at 461 (quoting S. REP. NO. 95-604 (1977), *reprinted in* 1978 U.S.C.C.A.N. 3904, 3916).

113. 50 U.S.C. § 1802(a)(1) (2000). The Act authorizes the President, through the Attorney General, to conduct electronic surveillance without a warrant if the Attorney General certifies under oath and in writing that:

> (A) the electronic surveillance is solely directed at (i) the acquisition of the contents of communications transmitted by means of communications used exclusively between or among foreign powers, . . . (ii) the acquisition of technical intelligence, other than the spoken communications of individuals, from property or premises under the open and exclusive control of a foreign powers . . . (B) there is no substantial likelihood that the surveillance will acquire the contents of any communication to which a United States person is a party; and (C) the proposed minimization procedures [are in place].

Id. Accord § 1822(a)(1) (authorizing warrantless physical searches under essentially the same circumstances).

114. *See* 28 C.F.R. § 501.3 (2003). If the requirements of § 1802(a)(1) or § 1822(a)(1) are met, warrantless monitoring is expressly authorized by statute and, presumably, the Attorney General would not need to rely upon § 501.3(d). *See supra* note 113.

Federal officers are authorized to apply for an order[115] under FISA "if the target of the electronic surveillance is a foreign power or an agent of a foreign power."[116] The FISA application must be supported by probable cause that the target of the surveillance is a foreign power or agent of a foreign power.[117] There must also be probable cause to believe that the "places at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power."[118] Importantly, the Act does not impose a requirement of probable cause to believe that a crime has been or is about to be committed.[119] The application must include certifications that:

> [T]he information sought [is deemed] to be foreign intelligence information; . . . the purpose of the surveillance is to obtain

---

115. There is some debate regarding whether a FISA order is a "warrant" contemplated by the Fourth Amendment. *See In re Sealed Case*, 310 F.3d at 737. In the first appeal from an order of the FISA Court, the FISA Court of Review acknowledged that there is no definitive answer to the question of whether FISA, as amended by the Patriot Act, meets the minimum Fourth Amendment warrant standards. *Id.* at 746. However, it held FISA constitutional because surveillance authorized by the Act is reasonable. *Id.* at 746 (relying on dicta and balancing test in United States v. United States Dist. Court (Keith), 407 U.S. 297 (1972)).

116. 50 U.S.C. § 1804(a)(4)(A) (2000). "Foreign power" means:

> (1) a foreign government or any component thereof, whether or not recognized by the United States; (2) a faction of a foreign nation or nations, not substantially composed of United States persons; (3) an entity that is openly acknowledged by a foreign government or governments to be directed and controlled by such foreign government or governments; (4) a group engaged in international terrorism or activities in preparation thereof; (5) a foreign-based political organization, not substantially composed of United States persons; or (6) an entity that is directed and controlled by a foreign government or governments.

§ 1801(a). "Agent of a foreign power" includes any person "who knowingly engages in sabotage or international terrorism, or activities that are in preparation thereof, for or on behalf of a foreign power." § 1801(b)(2)(C). This definition includes a United States citizen or permanent resident who "knowingly engages in clandestine intelligence gathering activities for or on behalf of a foreign power, which activities involve or may involve a violation of the criminal statutes of the United States." § 1801(b)(2)(A). "United States person" means a United States citizen, "an alien lawfully admitted for permanent residence . . . , an unincorporated association a substantial number of members of which are citizens of the United States or aliens lawfully admitted for permanent residence, or a corporation which is incorporated in the United States." § 1801(i).

117. § 1805(a)(3)(A). However, "no United States person may be considered a foreign power or an agent of a foreign power solely upon the basis of activities protected by the First Amendment to the Constitution of the United States." *Id.*

118. § 1805(a)(3)(B).

119. *See* § 1805(a), (b). But note that to find that a United States person is an "agent of a foreign power," there must be a finding that the person is engaged in activities that involve or may involve criminal conduct. *See* § 1801(b)(2)(A).

> foreign intelligence information;[120] that such information cannot reasonably be obtained by normal investigative techniques; that designates the type of foreign intelligence information being sought according to the categories described in [the Act]; and including a statement of the basis for the [last two] certification[s listed above].[121]

The Attorney General is required to approve the application before it is submitted to a FISA court judge,[122] who shall enter an *ex parte* order that approves the application if it meets the statutory requirements.[123]

Section 1822(b) authorizes applications for orders approving physical searches of "the premises, property, information, or material of a foreign power or an agent of a foreign power for the purpose of collecting foreign intelligence information."[124] Applications for a physical search order must be approved by the Attorney General and must include "the

---

120. One of the many ways in which the Patriot Act amended FISA was by changing the standard for obtaining an order. Previously, courts had interpreted FISA to allow an order to be issued only if the *primary* purpose of the surveillance was to obtain foreign intelligence information. *See In re Sealed Case*, 310 F.3d at 723-27. As amended, gathering foreign intelligence information need only be a *significant* purpose of the surveillance. *Id.* at 723; *see also* 50 U.S.C.A. § 1804(a)(7)(B) (2002). This change has sparked sharp criticism. Some commenters argue that this change allows surveillance to be conducted when the primary purpose is law enforcement and not foreign intelligence gathering. *See* Michael P. O'Connor & Celia Rumann, *Going, Going, Gone: Sealing the Fate of the Fourth Amendment*, 26 FORDHAM INT'L L.J. 1234, 1258 (2003) (characterizing the FISA Review Court's opinion in *In re Sealed Case* as approving the use of FISA orders when the government's primary purpose is law enforcement and arguing that this use of FISA orders violates the Fourth Amendment); Heath H. Galloway, *Don't Forget What We're Fighting For: Will the Fourth Amendment Be a Casualty of the War on Terror?* 59 WASH. & LEE L. REV. 921, 963-64 (2002) (examining the Fourth Amendment implications of various provisions of the Patriot Act, including the amendments to FISA).

121. 50 U.S.C. § 1804(a)(7). The certifications may be made "by the Assistant to the President for National Security Affairs or an executive branch official or officials designated by the President from among those executive officers employed in the area of national security or defense and appointed by the President with the advice and consent of the Senate." *Id.* Furthermore, the application must contain statements of the means by which the surveillance will be conducted; whether physical entry is required; facts concerning all previous applications made to any judge under the Act for the same persons, facilities or places; "the period of time for which the electronic surveillance is required to be maintained"; and, when more than one surveillance device is to be used, "the coverage of the devices involved and what minimization procedures apply to information acquired by each device." § 1804(a)(8)-(11). "Minimization procedures" are defined in the Act as specific procedures designed to minimize the acquisition, retention, and dissemination of nonpublic information during the course of the surveillance. §§ 1801(h), 1805(a)(4).

122. § 1805(a)(1). The FISA court consists of eleven district court judges from seven of the United States judicial circuits, designated by the United States Supreme Court Chief Justice. § 1803(a) (2003).

123. § 1805(a).

124. § 1822(b).

identity . . . or a description of the target of the search, and a detailed description of the premises or property to be searched and of the information, material or property to be seized, reproduced, or altered."[125] Applications must also include a statement of the facts relied upon to justify the search, including the belief that the target is a "foreign power or an agent of a foreign power," and that foreign intelligence information is on the property to be searched.[126] There also must be a "statement of the nature of the foreign intelligence sought," how the search will be conducted, "and a statement of minimization procedures."[127]

The judge shall enter an *ex parte* order approving the physical search if the judge finds that the application was authorized by the President, submitted by a federal officer, approved by the Attorney General, and included the appropriate minimization procedures and all of the required statements and certifications.[128] The judge must also find probable cause to believe that the target of the search is a foreign power or an agent of a foreign power, and that the premises or property to be searched is owned or used, possessed by, or is in transit to or from a foreign power or its agent.[129] Probable cause may be based, in part, on the past activities of the target "as well as facts and circumstances relating to current or future activities of the target."[130] Section 1824(e) allows warrantless searches in an emergency, but an application must be filed within seventy-two hours of the Attorney General's authorization.[131]

D. Obtaining Warrants to Monitor Inmate-Attorney Communications under Title III, FISA, and FED. R. CRIM. P. 41

If the Attorney General believes that an inmate is using or intends to use communications with his or her attorneys to facilitate acts of terrorism, a warrant or order may be obtained and surveillance initiated

---

125. § 1823(a)(3). The application must also include "(1) the identity of the Federal officer making the application; [and] (2) the authority conferred on the Attorney General by the President and approval of the Attorney General to make the application." § 1823(a)(1), (2).

126. § 1823(a)(4).

127. § 1823(a)(5), (6). Additionally, a qualified executive official must certify that: (1) the information sought is foreign intelligence information, (2) "a significant purpose of the search is to obtain foreign intelligence information," and (3) the information "cannot reasonably be obtained using normal investigative techniques." § 1823(a)(7) (2003). The certification must also designate the type of information sought. *Id.*

128. § 1824(a).

129. § 1824(a)(3). The statute provides that "[n]o United States person may be considered an agent of a foreign power solely upon the basis of activities protected by the [F]irst [A]mendment to the Constitution of the United States." *Id.*

130. § 1824(b).

131. 18 U.S.C. §§ 2516(1), 2518(3)(a) (2000).

under Title III, FED. R. CRIM. P. 41, or FISA, depending on whether the threat is from a domestic source or an agent of a foreign power, and depending on the anticipated type of monitoring.

In the case of domestic threats, the Attorney General may seek a warrant under Title III to conduct electronic surveillance by presenting the required application to a magistrate.[132] This is undoubtedly more burdensome than initiating monitoring under § 501.3(d), because Title III requires prior judicial approval and the probable cause standard in the statute is higher than the reasonable suspicion standard in the regulation. However, in light of the government's vast experience in seeking such warrants and the small number of inmates and warrants at issue, the burden is not unreasonable.[133] Moreover, requiring judicial approval has the benefit of providing a check on the power of the executive branch.

The government may obtain a warrant under FED. R. CRIM. P. 41 to seize written communications.[134] If reasonable cause is shown, the government may even obtain a "sneak and peek" warrant to covertly review or photograph the communications while delaying notification of the warrant's execution.[135] A warrant under Rule 41 also requires probable cause, but if probable cause is shown, the judge or magistrate has no discretion to refuse to issue the warrant.[136]

A FISA warrant imposes a different burden on the Attorney General. If the threat is from a foreign power, then the Attorney General may apply to a FISA court judge for an electronic surveillance or physical search order.[137] If the judge finds probable cause to believe that the inmate is an agent of a foreign power, the government is not required separately to prove that a crime has been or is about to be committed.[138] As with Title III warrants, prior judicial approval is required but is not unduly burdensome, and is consistent with our constitutional system of checks and balances.[139]

Once a warrant or order is obtained, the government may monitor communications between the inmate and his or her attorneys, either

---

132. 50 U.S.C. § 1824(e) (2003).

133. *DOJ Hearings*, *supra* note 4 (statement of Attorney General John Ashcroft during Senate Judiciary Committee Hearings that as of December 6, 2001 only 16 inmates met the standard for monitoring).

134. FED. R. CRIM. P. 41(a)(2)(A).

135. *See* United States v. Villegas, 899 F.2d 1324, 1336-37 (2d Cir. 1990).

136. *See* FED. R. CRIM. P. 41(d) (stating that the judge or magistrate *must* issue the warrant if there is probable cause under paragraph (c)) (emphasis added).

137. 50 U.S.C. § 1804(a) (2000).

138. *See* § 1805(a)(3), (4).

139. *See* § 1805(a).

covertly or after informing the inmate of the surveillance. Measures must still be taken to protect the attorney-client privilege, and the Attorney General may use routine screening procedures for searching and seizing attorney-client communications pursuant to warrants.[140] In light of these congressionally approved methods of conducting surveillance, no justification exists for the BOP monitoring regulation.

III. NATIONAL SECURITY AND THE WARRANT REQUIREMENT

Undoubtedly, warrantless monitoring as outlined in 28 C.F.R. § 501.3(d) is unconstitutional outside of the prison context.[141] The use of electronic devices to intercept attorney-client communications implicates the Fourth Amendment's warrant requirement, and courts have discussed extensively the government's duty to comply with the Fourth Amendment in the face of threats to national security,[142] although they have not defined the scope of the Executive's authority when faced with national security threats inside federal prisons. However, applying the reasoning from the decided cases, the Attorney General's assertion that warrantless monitoring is necessary to protect national security is unfounded.

A. Historic Overview of Executive Authority and the Warrant Requirement in Matters of National Security

Article II of the United States Constitution charges the President with the duty to "preserve, protect and defend the Constitution of the United States."[143] This includes the authority to protect the government against unlawful overthrow or subversion.[144] In the nation's early days, presidents exercised this authority by personally assuming responsibility for intelligence matters. Although Congress began enacting legislation

---

140. *See* United States v. Zolin, 491 U.S. 554, 556-57, 568 (1989) (approving the use of *in camera* review to determine whether allegedly privileged attorney-client communications fall within the crime-fraud exception, but only after the party opposing the privilege presents evidence sufficient to support a reasonable belief that the *in camera* review will yield evidence that the crime-fraud exception applies); United States v. Triumph Capital Group, Inc., 211 F.R.D. 31, 42-43 (D. Conn. 2002) (addressing proper procedures to protect privileged communications when a search involves property of an attorney, and citing U.S. Department of Justice's Guidelines for searches of the premises of attorneys).

141. *See* 18 U.S.C. § 2511 (2000); United States v. United States Dist. Court (Keith), 407 U.S. 297, 321 (1972); Berger v. New York, 388 U.S. 41, 51 (1967); *supra* Part II.

142. *E.g.*, United States v. Bianco, 998 F.2d 1112, 1124 (2d Cir. 1993) (citing *Berger*, the court held "[t]he interception of an oral conversation falls within the [F]ourth [A]mendment's protections, . . . and capturing a conversation through the use of electronic devices is a 'search and seizure'").

143. U.S. CONST. art. II, § 1.

144. *Keith*, 407 U.S. at 310.

and taking a more active role in intelligence in the twentieth century, presidents continued to authorize surveillance-particularly electronic surveillance-in national security matters, without prior judicial approval.[145] Presidents claimed such authority for decades until the Supreme Court held that the Fourth Amendment applied to electronic surveillance, thereby raising the question of the constitutionality of such warrantless surveillance.[146]

B. The Fourth Amendment Applies in the Face of Domestic Threats

The Supreme Court ruled more than thirty years ago that the President, acting through the Attorney General, is not exempt from the Fourth Amendment warrant requirement, even in cases involving threats to national security from domestic organizations.[147] In *United States v. United States District Court (Keith)*, three defendants were charged with conspiracy to destroy government property, and one of those defendants was charged with bombing a Central Intelligence Agency office in Ann Arbor, Michigan.[148] The Government admitted that the Attorney General had approved wiretaps "to gather intelligence information deemed necessary to protect the nation from attempts of domestic organizations to attack and subvert the existing structure of the Government."[149] The surveillance was conducted without prior judicial approval.[150] During the surveillance, agents overheard a conversation involving the defendant charged with the bombing.[151]

The government argued that the warrantless surveillance was a reasonable exercise of the President's inherent power to protect national security, and that Title III exempted national security surveillances from the Act's warrant requirement.[152] In an opinion authored by Justice

---

145. *See Keith*, 407 U.S. at 299; William C. Banks & M.E. Bowman, *Executive Authority for National Security Surveillance*, 50 AM. U.L. REV. 1, 48 (2000).

146. *See* Banks & Bowman, *supra* note 145 (citing Katz v. United States, 389 U.S. 347, 358 (1967)).

147. *Keith*, 407 U.S. at 320.

148. *Id.* at 299.

149. *Id.* at 300 (quoting the Attorney General's affidavit).

150. *Id.* at 301.

151. *Id.* at 300-01.

152. *Id.* at 303. The government relied on 18 U.S.C. § 2511(3) of Title III, which stated:

> Nothing contained in this chapter . . . shall limit the constitutional power of the President to take such measures as he deems necessary to protect the nation against actual or potential attack or other hostile acts of a foreign power, to obtain foreign intelligence information deemed essential to the security of the United States, or to protect national security information against foreign intelligence activities. Nor shall anything contained in this chapter be deemed to limit the constitutional power of the President to take such measures as he deems

Powell, the Supreme Court held that Title III did not confer any such power, but merely provided that the Act should "not be interpreted to limit or disturb such power as the President may have under the Constitution."[153] Consequently, any Executive authority to conduct warrantless searches in cases involving national security must be grounded in the President's constitutional powers.[154]

The Court was careful to note that it was not passing judgment on the President's power to conduct warrantless surveillance of foreign powers, or to obtain foreign intelligence.[155] According to the Attorney General, the surveillance in *Keith* was necessary to protect the nation from attack by domestic organizations. There was no evidence of any involvement of a foreign power.[156] Thus, the Court's sole concern was the President's alleged exemption from the Fourth Amendment warrant requirement in the face of threats from domestic organizations.[157]

The Court acknowledged the President's duty to protect the government from unlawful overthrow and the necessity of using electronic surveillance to gather intelligence regarding potential threats.[158] However, the Court recognized that this need had to be weighed against the potential for abuse:[159]

> If the legitimate need of Government to safeguard domestic security requires the use of electronic surveillance, the question is whether the needs of citizens for privacy and free expression may not be better protected by requiring a warrant before such

---

necessary to protect the United States against the overthrow of the Government by force or other unlawful means, or against any other clear and present danger to the structure or existence of the Government.

Id. at 302. Section 2511(3) was deleted in 1978 when the Act was amended and FISA was enacted. Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, 92 Stat. 1783; *see also* Halperin v. Kissinger, 606 F.2d 1192, 1202 n.66 (D.C. Cir. 1979).

153. *Keith*, 407 U.S. at 303. The Court noted that the language and legislative history of § 2511(3) refuted the government's interpretation. *Id.* The Court concluded, "We therefore think the conclusion inescapable that Congress only intended to make clear that the Act simply did not legislate with respect to national security surveillances." *Id.* at 306.

154. *Id.* at 308. The Court articulated the question as "[w]hether safeguards other than prior authorization by a magistrate would satisfy the Fourth Amendment in a situation involving the national security . . . ." *Id.* at 309 (quoting Katz v. United States, 389 U.S. 347, 358 n.23 (1967)).

155. *Id.* at 308.

156. *Id.* at 309 (quoting the Attorney General's affidavit).

157. *Id.* The Court noted that it often may be difficult to distinguish between domestic and foreign threats against the Government of the United States, but had no such difficulty in that case. *Id.* at 309 n.8.

158. *Id.* at 310. The Court said, "[i]t would be contrary to the public interest for the Government to deny to itself the prudent and lawful employment of those very techniques which are employed against the Government and its law-abiding citizens." *Id.* at 312.

159. *See id.* at 314-15.

> surveillance is undertaken. We must also ask whether a warrant requirement would unduly frustrate the efforts of Government to protect itself from acts of subversion and overthrow directed against it.[160]

The Court emphasized that the Fourth Amendment warrant clause was neither dead language, nor "an inconvenience to be somehow 'weighed' against the claims of police efficiency."[161] On the contrary, the warrant clause—with its requirements of probable cause and issuance by a neutral, disinterested magistrate—is a necessary safeguard against well-meaning but overly zealous executive officers.[162]

The Court further stated that "[t]hese Fourth Amendment freedoms cannot properly be guaranteed if domestic security surveillances may be conducted solely within the discretion of the Executive Branch."[163] Executive officers are charged with the duty to enforce the laws, to investigate, and to prosecute.[164] As such, they cannot serve as neutral or disinterested judges of their own enforcement, investigative, or prosecutorial efforts.[165] Nor is post-surveillance judicial review an acceptable check on executive discretion.[166] Instead, the Court favored prior review as the "time-tested" and appropriate means of assuring compliance with the Fourth Amendment.[167] The Court also rejected the argument that obtaining a warrant would be unduly burdensome.[168]

Finally, the Court was not swayed by arguments that a warrant is not required when criminal prosecution is the objective of the surveillance.[169] The government contended that the surveillance at issue in that case was conducted for the primary purpose of gathering intelligence about subversive forces and not for gathering evidence for a specific prosecution, and it claimed that the traditional warrant requirement should not apply in those circumstances.[170] The Court disagreed, noting that government surveillance risks infringement of constitutionally

---

160. *Id.* at 315.

161. *Id.* (quoting Coolidge v. New Hampshire, 403 U.S. 443, 481 (1971)).

162. *Id.*

163. *Id.* at 316-17.

164. *Id.* at 317.

165. *Id.* The Court noted, "The historical judgment, which the Fourth Amendment accepts, is that unreviewed executive discretion may yield too readily to pressures to obtain incriminating evidence and overlook potential invasions of privacy and protected speech." *Id.*

166. *Id.* Indeed, the court noted that no such review would ever take place if the government declined to prosecute. *Id.* at 318.

167. *Id.* at 318.

168. *Id.* at 318-21.

169. *Id.* at 318-20.

170. *Id.* at 318-19.

protected privacy, regardless of its purpose.[171] "We recognize, as we have before, the constitutional basis of the President's domestic security role, but we think it must be exercised in a manner compatible with the Fourth Amendment. In this case we hold that this requires an appropriate prior warrant procedure."[172]

The Court acknowledged that domestic security surveillance might involve different practical and policy considerations than those involved in surveillance of "ordinary crime" and invited Congress to set standards appropriate for issuing warrants in cases of threats to domestic security.[173] The Court noted that standards different from those set out in Title III:

> may be compatible with the Fourth Amendment if they are reasonable both in relation to the legitimate need of Government for intelligence information and the protected rights of our citizens. For the warrant application may vary according to the governmental interest to be enforced and the nature of citizen rights deserving protection.[174]

C. *FISA Applies in the Face of Threats to National Security from Agents of Foreign Powers*

In *Keith*, the Court expressly declined to decide whether the President had inherent constitutional authority to conduct warrantless electronic surveillance to obtain foreign intelligence information in the interest of national security.[175] The courts of appeals were divided on the answer to that question. The Third and Fifth Circuits sustained the President's power to conduct warrantless electronic surveillance for the primary purpose of gathering foreign intelligence information,[176] but the D.C. Circuit held that a cause of action was stated under the Fourth Amendment for damages resulting from warrantless surveillance, even

---

171. *Id.* at 320. The Court further noted the especially sensitive nature of security surveillances, citing the "inherent vagueness of the domestic security concept, the necessarily broad and continuing nature of intelligence gathering, and the temptation to utilize such surveillances to oversee political dissent." *Id.*

172. *Id.* at 320. In its opinion, the Court acknowledged that there have been a few, carefully delineated exceptions to the warrant requirement. *Id.* at 318. However, those exceptions were recognized in cases in which there is a need for law enforcement officers to protect their own well-being and preserve evidence from destruction. *Id.* Even when the Court has recognized those exceptions, it has consistently reaffirmed the principle that police must obtain a warrant whenever practicable. *Id.* (citing Terry v. Ohio, 392 U.S. 1, 20 (1968); Chimel v. California, 395 U.S. 752, 762 (1969)).

173. *Id.* at 322.

174. *Id.* at 322-23.

175. *Id.* at 308.

176. United States v. Butenko, 494 F.2d 593, 605 (3d Cir. 1974) (en banc), *cert. denied,* 419 U.S. 881 (1974); United States v. Brown, 484 F.2d 418, 426 (5th Cir. 1973), *cert. denied,* 415 U.S. 960 (1974).

though the Attorney General had approved the surveillance for the purpose of gathering foreign intelligence information.[177] Soon after *Keith* was decided, Congress resolved this conflict by enacting FISA, which includes standards for foreign intelligence surveillance orders that vary from the warrant standards in Title III.[178] Congress, through its enactment of FISA, "sought to resolve doubts about the constitutionality of warrantless, foreign security surveillance and yet protect the interests of the United States in obtaining vital intelligence about foreign powers."[179] FISA allows electronic surveillance of foreign agents without the necessity of establishing probable cause that a crime has been or will be committed.[180] Thus, Congress apparently concluded that the inquiry for determining the reasonableness of a search under the Fourth Amendment depends on whether foreign agents are targets.[181]

Notably, some courts, including the FISA Court of Review, continue to assume that the President has inherent authority to conduct warrantless searches for the purpose of obtaining foreign intelligence.[182] The Supreme Court has not ruled on this precise question, but its

177. Zweibon v. Mitchell, 516 F.2d 594, 607, 659, 669 (D.C. Cir. 1975) (en banc), *cert. denied,* 425 U.S. 944 (1976).

178. *Compare* the Title III warrant standards, 18 U.S.C. § 2518 (2000), *with* requirements for FISA order, 50 U.S.C. § 1805 (2000).

179. ACLU Found. of S. Cal. V. Barr, 952 F.2d 457, 461 (D.C. Cir. 1991).

180. 50 U.S.C. § 1805(a).

181. *See In re Sealed Case*, 310 F.3d 717, 738 (Foreign Int. Surv. Ct. Rev. 2002) (noting the different standards for obtaining a warrant under Title III and FISA). The court stated:

> Congress clearly intended a lesser showing of probable cause for these activities than that applicable to ordinary criminal cases . . . . And with good reason—these activities present the type of threats contemplated by the Supreme Court in *Keith* when it recognized that the focus of security surveillance "may be less precise than that directed against more conventional types of crime" even in the area of *domestic* threats to national security.

Id. This approach follows the Supreme Court's language in *Keith* suggesting that standards for national security surveillance warrants might differ from those in Title III. United States v. United States Dist. Court (Keith), 401 U.S. 297, 322 (1972).

182. *In re* Sealed Case, 310 F.3d at 742. The FISA Court of Review noted that courts that have decided the issue have held that the President has inherent authority to conduct warrantless searches to obtain foreign intelligence information (although all of the cases cited were decided before FISA was enacted). *Id.* "We take for granted that the President does have that authority and, assuming that is so, FISA could not encroach on the President's constitutional power." *Id. See generally* William F. Brown & Americo R. Cinquegrana, *Warrantless Physical Searches for Foreign Intelligence Purposes: Executive Order 12,333 and the Fourth Amendment*, 35 CATH. U. L. REV. 97 (1985) (examining constitutional justification for presidential authority to conduct warrantless searches for foreign intelligence purposes); David S. Eggert, *Executive Order 12,333: An Assessment of the Validity of Warrantless National Security Searches*, 1983 DUKE L.J. 611, 634-35 (1983) (arguing that whatever authority the President has to conduct foreign intelligence surveillance, the surveillance must comply with the Fourth Amendment).

reasoning in *Keith*, along with the enactment of FISA and Congress's statement in 18 U.S.C.A. § 2511(f) that the procedures in Title III and FISA "shall be the exclusive means by which electronic surveillance . . . and the interception of wire and oral communications may be conducted," strongly indicate that the President's inherent authority to conduct warrantless searches is very narrow, if it exists at all.[183] In any event, § 501.3(d) clearly authorizes warrantless searches and seizures that are not conducted for purposes other than the obtaining of foreign intelligence. Consequently, those searches and seizures do not fall within whatever inherent authority the President may have.

D. The Regulation is not a Valid Exercise of the President's Authority as Commander in Chief

The Executive's authority as Commander in Chief does not justify the abrogation of rights permitted by the regulation. While the courts have been extremely deferential to the Executive when addressing confinement and trial of suspected terrorists,[184] the deference is not unlimited. In the current "war on terrorism," the courts have been most deferential to the President in his capacity as Commander in Chief.[185] Courts appear particularly reluctant to question the President's judgment with respect to the detention of enemy combatants during a time of war.[186] However, § 501.3(d) would apply in times of peace to inmates who have never taken up arms against America and who have not been designated as enemy combatants.[187] Under these circumstances, the same degree of deference to the Executive is unwarranted.

---

183. *See* Banks & Bowman, *supra* note 145 (discussing the remaining constitutional issue regarding the Executive's authority to conduct warrantless searches in light of the amended language of Title III). The Second Circuit recently expounded upon the limits of the President's inherent authority in *Padilla v. Rumsfeld*, 352 F.3d 695 (2d Cir. 2003) (*Padilla IV*). *See infra*, Part III.D. The court noted that when the President acts in a manner contrary to congressionally enacted legislation, the President's authority is at its "lowest ebb." *Padilla*, 352 F.3d at 711 (quoting Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579, 637 (Jackson, J., concurring)). The court qualified the decision by stating that "Courts can sustain exclusive presidential control [in this situation] only by disabling the Congress from acting upon the subject." *Youngstown*, 343 U.S. at 637-38.

184. Hamdi v. Rumsfeld, 296 F.3d 278, 281 (4th Cir. 2002) (noting that in the area of foreign relations and national security, courts give considerable deference to the political branches).

185. *See, e.g., id*; Hamdi v. Rumsfeld, 316 F.3d 450, 463 (4th Cir. 2003) (Hamdi II); Padilla v. Bush, 233 F. Supp. 2d 564, 589 (S.D.N.Y. 2002).

186. *See Padilla*, 233 F.3d at 588-89. The court noted that no formal declaration of war is necessary for the President to use his power as Commander in Chief. *Id.* at 588-90; *see also Hamdi II*, 316 F.3d at 466.

187. 28 C.F.R. § 501.3 (2002).

Judicial deference is due largely to the Constitution's allocation of powers.[188] Article II, section 2 declares that the President shall be the Commander in Chief of the armed forces, and empowers the President to detain persons captured during armed conflicts, to deport or detain alien enemies during hostilities, and to confiscate and destroy enemy property.[189] The Court has held that "[t]he constitutional allocation of war powers affords the President extraordinarily broad authority as Commander in Chief and compels courts to assume a deferential posture in reviewing exercises of this authority."[190] Recently, several courts exercised such deference when individuals designated by the President as "enemy combatants" challenged the legality and conditions of their detention.[191]

The Fourth Circuit vacated a district court order directing the United States to allow a public defender to have unmonitored access to Yaser Esam Hamdi, an American citizen.[192] The United States had objected to the district court order and asserted that because Hamdi had been declared an "enemy combatant," he had "no general right under the laws and customs of war, or the Constitution . . . to meet with counsel concerning [his] detention, much less . . . without military authorities present."[193] The Fourth Circuit criticized the district court for failing to give proper weight to national security concerns and the effect of Hamdi's unmonitored access to counsel on the government's ongoing intelligence efforts.[194]

The Second Circuit examined the limits of the President's inherent authority in *Padilla v. Rumsfeld*.[195] In *Padilla*, the government argued that as Commander-in-Chief, "the President has the inherent authority

188. *Hamdi II*, 316 F.3d at 474.

189. U.S. CONST. art. II, § 2; *see also Hamdi II*, 316 F.3d at 463.

190. *Hamdi II*, 316 F.3d at 474.

191. *Id.*; *Padilla*, 233 F. Supp. 2d at 606.

192. Hamdi v. Rumsfeld, 296 F.3d 278, 282-83 (4th Cir. 2002) (*Hamdi I*).

193. *Id.* at 282.

194. *Id.* The order was reversed and remanded for further proceedings "[b]ecause the district court appointed counsel and ordered access to the detainee without adequately considering the implications of its actions and before allowing the United States even to respond." *Id.* at 284. This issue was not raised in *Hamdi II*. *See Hamdi II*, 316 F.3d at 466 n.4. Thus, the Fourth Circuit has not had to decide whether enemy combatants can be held without access to counsel. The United States Supreme Court granted Hamdi's petition for writ of certiorari challenging the Fourth Circuit's judgements. 124 S. Ct. 981 (2004). The Department of Defense subsequently announced that Hamdi would be granted access to a lawyer but reiterated their belief that the decision was discretionary and not legally required. P. Jess Bravin, *White House to Allow Counsel For U.S.-Born Taliban Detainee*, WALL ST. J., Dec. 3, 2003, at A5.

195. 352 F.3d 695, 699 (2d Cir. 2003) (Padilla IV).

to detain those who take up arms against this country."[196] In response, Padilla, an American citizen, contended that the President's actions were in conflict with the Non-Detention Act, which prohibits detention of American citizens absent express congressional authorization.[197] By designating Padilla an enemy combatant and detaining him without congressional authorization, the President impermissibly "engaged in the 'lawmaking' function entrusted by the Constitution to Congress in violation of the separation of powers."[198]

The court agreed that the order to detain Padilla as an enemy combatant was legislative in nature and consequently outside of the President's authority as Commander-in-Chief. The court cited the Offenses Clause, the Suspension Clause, and the Third Amendment as examples of the Constitution's explicit grant of power to Congress to make laws affecting individual liberties in times of war.[199] Noting that the Framers understood that individual liberties may be abridged in times of national crisis, the court concluded: "the inherent emergency powers necessary to effect such abridgements" rest with Congress, not the President.[200] Thus, "while Congress—otherwise acting consistently with the Constitution—may have the power to authorize the detention of United States citizens under the circumstances of Padilla's case, the President, acting alone, does not."[201]

These two cases demonstrate the deference given to the President with respect to detention of suspected terrorists and the limits of that deference.[202] It is Congress's role to enact legislation affecting individual liberties domestically, even in times of war. Section 501.3(d), enacted without congressional approval and contrary to the provisions of Title III, FISA, and Federal Rule of Criminal Procedure 41, affects the individual liberties of federal inmates arrested and imprisoned domestically.[203] In these circumstances, the President cannot rely on his authority as Commander-in-Chief to deprive inmates of their constitutional rights.

---

196. *Id.* at 712 (citing U.S. CONST. art. II, § 2).

197. *Id.* at 713.

198. *Id.*

199. *Id.* at 715.

200. *Id.* at 714 (citing Youngstown Sheet Tube Co. v. Sawyer, 343 U.S. 579, 649-50 (Jackson, J., concurring)). Padilla argued that Congress has never defined the term "enemy combatant," or stated when that term applies, and claimed: "The President's order does not direct that a congressional policy be executed in a manner prescribed by Congress—it directs that a presidential policy be executed in a manner prescribed by the president." *Id.* at 714 (citing *Youngstown*, 343 U.S. at 588).

201. *Id.* at 715.

202. *See id.*; *Hamdi II*, 316 F.3d at 474.

203. *See* 28 C.F.R. § 501.2(d) (2002).

E. National Security and Warrants (or Not) Inside of Prisons

The Supreme Court considered and rejected the argument that the President is exempt from the Fourth Amendment warrant requirement when faced with domestic threats to national security.[204] In reaching this decision, the Supreme Court carefully considered the potential impact on national security and the burden that the warrant requirement places on the Executive.[205] Ultimately, the Court concluded that even pressing national security concerns do not justify a complete exemption from the requirement of prior judicial approval.[206] Consequently, absent exceptional circumstances,[207] federal law enforcement officials cannot monitor the communications between a suspected domestic terrorist and his or her attorney outside of the prison context without a warrant.

Yet, the Attorney General argues that national security demands that he have the authority to monitor that same suspect without a warrant once that suspect is arrested and becomes a federal inmate. In support of this argument, the Attorney General cites an al Qaeda training manual that advises imprisoned members to hide messages to communicate and exchange information with members outside of prison.[208] In light of this evidence that certain imprisoned terrorists may intend to further their unlawful aims using any means of communication possible—even by passing hidden messages through an unwitting attorney—the Attorney General claims that the new rule is a necessary measure to prevent future terrorist attacks.[209]

This argument is logically flawed. A suspected terrorist outside of prison has the ability to contact co-conspirators directly and freely. If the Attorney General suspects that an individual who is not an inmate is planning a terrorist attack, no surveillance could take place without prior court authorization.[210] After carefully considering this issue, both Congress (by enacting FISA) and the Supreme Court (in *Keith*) concluded that national security can be protected even if the Executive is required to obtain a warrant before conducting surveillance.[211] No reason has been articulated for the proposition that inmates—whose *only* potential link to their network of terror is through their attorneys—

---

204. United States v. United States Dist. Court (Keith) 407 U.S. 297, 320-21 (1972).

205. *Id.*

206. *Id.* at 321.

207. *See id.* at 318.

208. *DOJ Hearings*, *supra* note 4 (statement of Attorney General John Ashcroft).

209. *See id.*

210. Except, of course, in case of emergency circumstances as defined in case law or statutes. *See, e.g.*, 18 U.S.C. § 2518(7) (2000).

211. *See* 50 U.S.C. § 1805(f); United States v. United States Dist. Court (Keith), 407 U.S. 321 (1972).

would pose a greater risk to national security than suspected terrorists outside of federal prisons.

Nor is there any evidence that requiring the Attorney General to obtain a warrant before monitoring attorney-client communications would constitute an undue burden, particularly in light of testimony that only a handful of inmates are currently subject to monitoring.[212] Requiring a warrant will only prevent monitoring in those circumstances in which the Attorney General is unable to convince a neutral and detached magistrate that probable cause exists to believe that the inmate will use his or her communications with the attorney to further acts of terrorism.[213] But this is precisely the point of prior judicial review: preventing the Executive from exercising sole discretion in conducting searches.[214] The magistrate or judge represents the judicial check on the power of the Executive Branch; and in the end "[a]lthough some added burden will be imposed upon the Attorney General, this inconvenience is justified in a free society to protect constitutional values."[215]

Finally, existing rules and statutes give the Attorney General more flexibility with respect to disclosure of monitoring. While § 501.3(d) requires advance notice of monitoring, warrants can be obtained *ex parte* under Title III, FED. R. CRIM. P. 41, and FISA.[216] Nothing prevents the Attorney General from disclosing the surveillance if doing so better suits his purposes, but disclosure remains purely discretionary. Knowing that they might be subject to covert surveillance at any time—with or without notice to the inmate—arguably furthers the goal of deterrence more effectively than surveillance that alerts the inmate of the need to speak in code or hide messages to evade detection by the monitors.

While it is convenient to be able to monitor attorney-client communications of inmates without having to seek prior judicial approval, convenience is different from necessity. National security can be adequately protected by compliance with Title III, FED. R. CRIM. P. 41, or FISA, while preserving a vital check on the authority of the

---

212. *See DOJ Hearings*, *supra* note 4 (statement of Attorney General John Ashcroft) (stating that regulation only applied to sixteen people as of December 6, 2001).

213. The burden of proof would be higher as well, because under Title III the magistrate must find probable cause to believe that a crime has been, is being, or is about to be committed, while under 28 C.F.R. § 501.3(d) (2002), the Attorney General must only have a "reasonable suspicion . . . that a particular inmate may use communications with attorneys or their agents to further or facilitate acts of terrorism." § 501.3(d). However, the Attorney General has articulated no reason why the lower standard is necessary to protect national security.

214. *See Keith*, 407 U.S. at 316-17.

215. *See id.* at 321 (commenting on the holding that the government's concerns did not justify deviation from the Fourth Amendment requirement of prior judicial approval).

216. 50 U.S.C. § 1805(a) (2000); 18 U.S.C. § 2518 (2000); FED. R. CRIM. P. 41(d)(1).

executive branch and the sanctity of the attorney-client relationship. Vesting unchecked authority in one branch of government—indeed in one individual: the Attorney General—is not only antithetical to our system of checks and balances, but it sets the stage for abuses of authority by "well-intentioned but mistakenly over-zealous executive officers."[217] This danger becomes especially acute with § 501.3(d) because the initial decision to initiate monitoring is not subject to judicial review.[218] One cannot challenge the Attorney General's conclusion that a particular inmate is unlikely to use communications with his or her attorney to facilitate acts of terrorism. Nor can one challenge the privilege team's conclusions with respect to which communications fall outside of the attorney-client privilege, and therefore can be retained by the government, without notice to the inmate or attorney.[219] With respect to Section 501.3(d), such authority is both unnecessary and unwise.[220]

IV. INMATES' CONSTITUTIONAL RIGHTS

The Supreme Court has noted that "[p]rison walls do not form a barrier separating prison inmates from the protections of the

---

217. Coolidge v. New Hampshire, 403 U.S. 443, 481 (1971) (quoting Gouled v. United States, 255 U.S. 298, 304 (1921)).

218. *See* § 501.3(d). The inmate and attorney have the option of filing a lawsuit to challenge the legality of the regulation itself, but that is a very time-consuming and circuitous route that is not likely to prevent monitoring in the meantime. *See* § 501.3(e).

219. The regulation merely requires judicial approval before the information can be "disclose[d]" by the privilege team. § 501.3(d)(3). This does not prevent a member of the privilege team from indirectly using the information in other investigations. Furthermore, a significant risk exists that the privilege team will be unable to determine whether particular communications are privileged because the targeted inmates will likely be suspected of using codes or hidden messages to conceal a criminal purpose which could invoke the crime-fraud exception to the attorney-client privilege.

220. Abuse by BOP or DOJ officers may be the exception to the rule, but such abuses do occur. Section 1001 of the Patriot Act directs the Office of the Inspector General (OIG), U.S. Department of Justice to provide semiannual reports to Congress on claims of civil rights and civil liberties abuses by DOJ employees. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) Act of 2001, Pub. L. No. 107-56, § 1001, 115 Stat. 272, 391 (Oct. 26, 2001). In its July 17, 2003 report, the OIG received 1,073 complaints of Patriot Act-related civil rights or civil liberties abuses. U.S. Department of Justice Office of the Inspector General, Report to Congress on Implementation of Section 1001 of the USA PATRIOT Act, July 17, 2003 at 6. Of those, 272 were within the OIG's jurisdiction, and of the 272, thirty-four stated credible Patriot Act complaints. *Id.* While thirty-four may not seem like a large number, those complaints cover only a six month period of time (from December 16, 2002 through June 15, 2003). *See id.* While some complaints may prove unfounded, others will yield proof of abuses, as in the case of a BOP corrections officer who admitted to verbally abusing a Muslim inmate. *Id.* at 7.

Constitution."[221] Indeed, the Supreme Court has insisted that "prisoners be accorded those rights not fundamentally inconsistent with imprisonment itself or incompatible with the objectives of incarceration."[222] Among the rights that the Supreme Court has acknowledged as retained by inmates are the Eighth Amendment right to be free from cruel and unusual punishment, the Fifth Amendment right to due process, the First Amendment right to reasonable opportunities to practice their religion, and the right to petition the government for redress of grievances.[223] Federal courts are bound to protect these constitutional rights against infringement by prison regulations or practices.[224]

Section 501.3(d) implicates additional rights, including the Sixth Amendment right to counsel and the Fourth Amendment right to be free from unreasonable search and seizure. Possible violations of inmates' Fourth Amendment rights have received less attention and present a more complicated problem, given the limited privacy rights retained by prison inmates. But the right to confidential attorney-client communications is sufficiently important to give inmates a justifiable expectation of privacy in such communications, that is protected by the Fourth Amendment.

A. The Fourth Amendment and Inmates' Right to Privacy in Their Cells

The Fourth Amendment to the United States Constitution declares:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated; and no Warrants shall issue but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[225]

This Amendment "safeguard[s] the privacy and security of individuals against arbitrary invasions by governmental officials."[226] Central to Fourth Amendment analysis is determining when a "search" or "seizure" has occurred. The Supreme Court has relied upon the description in Justice Harlan's concurrence in *Katz v. United States*, which states that for Fourth Amendment purposes, "a search occurs when the government

221. Turner v. Safley, 482 U.S. 78, 84 (1987). *See also* Hudson v. Palmer, 468 U.S. 517, 523 (1984) ("We have repeatedly held that prisons are not beyond the reach of the Constitution.").

222. *Hudson*, 468 U.S. at 523.

223. *Id.* at 523; *Turner*, 482 U.S. at 84.

224. *Turner*, 482 U.S. at 84.

225. U.S. CONST. amend. IV.

226. Camara v. Municipal Ct., 387 U.S. 523, 528 (1967).

violates a subjective expectation of privacy that society recognizes as reasonable."[227]

Katz also clarified that the Fourth Amendment protects people, not places.[228] Although the wording of the Fourth Amendment is chiefly directed against intrusions into private homes, it is well established that it also "shields private speech from unreasonable surveillance."[229] Consequently, determining whether a search or seizure violates this constitutional provision requires more than determining whether a certain place is a "constitutionally protected area."[230] Instead, courts must determine whether the search or seizure violated the target's reasonable or justifiable expectation of privacy.[231] Several courts have therefore refused to hold that inmates lose all of their Fourth Amendment rights simply because they are in prison, although their status as inmates is highly relevant in assessing the reasonableness of their expectation of privacy.

Obviously, inmates lose most of their privacy rights while imprisoned. Thus it is clear that inmates are not entitled to the full panoply of Fourth Amendment protections. The precise scope of their remaining Fourth Amendment rights, on the other hand, is unclear. In *Hudson v. Palmer*, the Supreme Court held that inmates retain no reasonable expectation of privacy in their cells,[232] and the government relies on this holding to support its assertion that inmates retain no Fourth Amendment rights at all.[233] This assertion, however, greatly overstates the holding of *Hudson* and fails to take into account the reasoning behind the holding or the context in which it was decided. Furthermore, several courts have recognized that inmates, particularly pre-trial detainees, retain some residuum of privacy rights, even after *Hudson*.

Hudson involved the shakedown of an inmate's cell in a Virginia prison.[234] The inmate, Palmer, filed suit in federal district court under 42 U.S.C. § 1983, alleging that Hudson, an officer at the prison, had conducted an unreasonable search of his locker and cell, and had brought a false charge of destroying state property against him for the sole

227. *Id.* at 33 (citing United States v. Katz, 389 U.S. 347, 361 (1967) (Harlan, J. concurring)). The *Katz* rule has been criticized as circular and unpredictable. *Id.* at 34.

228. *See Katz*, 389 U.S. at 351.

229. United States v. United States Dist. Court (Keith), 407 U.S. 297, 313 (1972).

230. *See Katz*, 389 U.S. at 350-51.

231. *See id.* at 353.

232. 468 U.S. 517, 525-26 (1984).

233. *See* Richard G. Schott, *Warrantless Interception of Communications*, 72 FBI Law Enforcement Bulletin 25, 28 (January 2003) (citing *Hudson* and stating that there is no expectation of privacy in prisons).

234. Hudson v. Palmer, 468 U.S. 517, 519-20 (1984).

purpose of harassment.[235] Palmer further alleged that Hudson intentionally destroyed his property during the search, in violation of Palmer's Fourteenth Amendment right to due process.[236] The district court ruled for Hudson and the Fourth Circuit affirmed with respect to the due process claim, holding that Palmer was not deprived of his property without due process because an adequate post-deprivation state remedy existed.[237]

Nevertheless, the Fourth Circuit also held that "a prisoner has a 'limited privacy right' in his cell entitling him to protection against searches conducted solely to harass or to humiliate."[238] In order to protect this right, "shakedown" searches of a cell should be conducted only "'pursuant to an established program of conducting random searches . . . reasonably designed to deter or discover the possession of contraband' or upon reasonable belief that the prisoner possesses contraband."[239] The court remanded the case for a determination of the purpose of the search at issue.[240]

Both parties appealed, and the Supreme Court granted certiorari to determine, in part, whether inmates are entitled to the Fourth Amendment's protection from unreasonable searches and seizures in their cells.[241] The Supreme Court defined the inquiry as whether inmates have a justifiable expectation of privacy that has been violated by government action: "We must decide, in Justice Harlan's words, whether a prisoner's expectation of privacy in his prison cell is the kind of expectation that society is prepared to recognize as reasonable."[242] The Court answered this question in the negative.[243]

The Court pointed out that inmates, by definition, are individuals who have engaged in antisocial and often violent conduct, and have demonstrated an inability to control or conform their behavior to societal

---

235. *Id.* at 520.

236. *Id.*

237. *Id.* at 520-21 (citing the holding in Parratt v. Taylor, 451 U.S. 527 (1981), that a negligent deprivation of inmate's property by state officials does not violate his Fourteenth Amendment right to due process if an adequate post-deprivation state remedy exists and concluding that this holding should be extended to intentional deprivations of property).

238. *Id.* at 521 (quoting Bell v. Wolfish, 697 F.2d 1220, 1225 (1983)).

239. *Id* at 522-23 (quoting the court of appeals' majority opinion).

240. *Id.* at 522.

241. *Id.* at 519. The Court also granted certiorari to determine whether *Parratt's* holding regarding negligent deprivations of property should be extended to intentional deprivations of property. *Id.*

242. *Id.* at 525 (quoting Justice Harlan's concurring opinion in United States v. Katz, 389 U.S. 347, 360 (1967)).

243. *Id.* at 525-26.

expectations.[244] Additionally, the Court cited statistics on violent crime in the "volatile" state and federal prison systems and noted prison administrators' responsibility to ensure the safety of the prison staff, personnel, and visitors, in addition to the safety of the inmates themselves.[245] In particular, prison administrators face the daunting task of preventing drugs, weapons, and other contraband from entering or circulating in the prisons, and detecting escape plots before they occur, all while maintaining a sanitary environment.[246] The Court concluded that it would be "literally impossible" to maintain order and security if inmates retained a right of privacy in their cells: "Virtually the only place inmates can conceal weapons, drugs, and other contraband is in their cells. Unfettered access to these cells by prison officials, thus, is imperative if drugs and contraband are to be ferreted out and sanitary surroundings are to be maintained."[247]

This need to maintain security in penal institutions was balanced against the interests of inmates' privacy within their cells. The Court struck the balance in favor of prison security, which it had consistently identified as a central goal of correction systems.[248] The Court was confident that society would agree that loss of privacy is an inherent consequence of incarceration and therefore, the Court concluded that prisoners have no reasonable expectation of privacy in their prison cells.[249] Consequently, "the Fourth Amendment proscription against unreasonable searches does not apply within the confines of the prison cell."[250]

B. Inmate Privacy Rights After Hudson

While the holding in *Hudson* certainly reduced inmates' privacy rights, it did not foreclose the recognition of a right to privacy with respect to communications between inmates and their attorneys. Many courts have read the holding as depriving inmates of only some of their Fourth Amendment privacy rights,[251] because the *Hudson* Court carefully limited its discussion to the reasonable expectation of inmates *in their*

244. *Id.* at 526.
245. *Id.* at 526-27.
246. *Id.*
247. *Id.* at 527.
248. *Id.* (citing Pell v. Procunier, 417 U.S. 817, 823 (1974)).
249. *Id.* at 527-28.
250. *Id.* at 526.
251. *See, e.g.*, United States v. Cohen, 796 F.2d 20, 23 (2d Cir. 1986).

cells.[252] Moreover, the Court's conclusion that no privacy right existed in prison cells was based upon prison officials' need for unfettered access to the cells to search for contraband.[253] The Court did not address inmates' Fourth Amendment rights in relation to searches or seizures for purposes unrelated to institutional security.

Several courts have held that *Hudson* does not apply to searches of prison cells when the search is not related to prison security.[254] In *United States v. Cohen*,[255] the Second Circuit was asked to decide whether prison officials violated a pretrial detainee's Fourth Amendment rights when they searched his cell without a warrant.[256] Arthur Barr was arrested and charged with conspiracy to distribute cocaine in June 1984.[257] Unable to post bail, Barr was held in pretrial detention at the New York Metropolitan Correctional Center.[258] He was charged with distribution of cocaine and interstate travel in aid of drug distribution, operating a continuing criminal enterprise, tax evasion, obstruction of justice, and witness tampering.[259]

While Barr was incarcerated and awaiting trial, Assistant United States Attorney Michael R. Bromwich instructed prison officials to conduct a search of Barr's cell "to look for certain types of documents that may have contained the names and phone numbers of other of Barr's co-conspirators and witnesses who Barr had already contacted and was still . . . trying to contact."[260] Acting on Bromwich's instruction, one of the corrections officers conducted a "contraband" search of Barr's cell, which consisted solely of an examination of Barr's papers.[261] Based upon information found during this search, the government obtained a search warrant for Barr's cell authorizing the seizure of all of his written, non-

252. *Id.* at 530 (concluding that "prisoners have no legitimate expectation of privacy and that the Fourth Amendment's prohibition on unreasonable searches does not apply *in prison cells*") (emphasis added).

253. *Id.* at 527. This holding is consistent with the test in *Turner v. Safley*, decided three years after *Hudson*, in which the Court stated that prison regulations that impinge on inmates' constitutional rights will be upheld if they are reasonably related to legitimate penological interests. *See* Turner v. Safley, 482 U.S. 78, 89-90 (1987).

254. *See, e.g.*, United States v. Cohen, 796 F.2d 20 (2d Cir. 1986); State v. Henderson, 517 S.E.2d 61 (Ga. 1999) (concluding that "*Hudson* did not deprive pre-trial detainees of all Fourth Amendment protections"); McCoy v. State, 639 S.2d 163 (Fl. Dist. Ct. App. 1994).

255. 796 F.2d 20 (2d Cir. 1986).

256. *Id.* at 20, 21.

257. *Id.* at 21.

258. *Id.*

259. *Id.*

260. *Id.*

261. *Id.*

legal materials.[262] Pursuant to the warrant, the government seized papers that it sought to use against Barr at his trial.[263] Barr argued that the initial, warrantless search violated the Fourth Amendment, and moved to have the resulting evidence suppressed.[264] His motion was denied, and Barr appealed.[265]

The government claimed that *Hudson* controlled and required affirmance of the district court's judgment.[266] It argued that since neither convicted inmates nor pretrial detainees have any right of privacy in their cells, evidence obtained during a search of a prisoner's cell cannot be suppressed on constitutional grounds.[267] The Second Circuit rejected this argument; instead, it concluded that *Hudson* should not be read to hold that pre-trial detainees retain no Fourth Amendment rights regardless of the circumstances underlying the search.[268]

The court gave several reasons for its conclusion. First, the search was initiated at the request of the prosecution, with the hope of finding incriminating evidence, and not by prison officials motivated by safety concerns.[269] The Second Circuit noted that the Supreme Court did not have this situation in mind when deciding *Hudson*,[270] which emphasized the need to balance individual rights against "legitimate penological objectives."[271]

While acknowledging prison officials' need for discretion to take measures to ensure prison security, the court declined to extend that discretion to prosecutors.[272] Because the purpose of the prosecution's search was solely to obtain information for another indictment, the court that the type of search was outside of the scope of *Hudson*.[273] The court

---

262. *Id.*

263. *Id.* at 21, 23.

264. *Id.* at 21.

265. *Id.*

266. *Id.* at 22.

267. *Id.*

268. *Id.* at 23.

269. *Id.* (noting that the decision was not made by those officials in the best position to evaluate security needs, "nor was the search even colorably motivated by institutional safety concerns").

270. *Id.* The court explained:

> The Supreme Court in *Hudson* did not contemplate a cell search intended solely to bolster the prosecution's case against a pre-trial detainee awaiting his day in court; it did not have before it the issue of whether such a search could lawfully be used by government prosecutors to uncover information that would aid them in laying additional indictments against a detainee.

Id.

271. *Id.*

272. *Id.* at 23-24.

273. *Id.* at 24.

held that Barr retained an expectation of privacy in his cell sufficient to challenge the warrantless search requested by the prosecution on Fourth Amendment grounds.[274]

Courts have also recognized that prisoners "retain a limited constitutional right to bodily privacy, particularly as to searches viewed or conducted by members of the opposite sex."[275] In *Hayes*, the Tenth Circuit held that summary judgment in favor of prison administrators was inappropriate in a case in which an inmate alleged that he had been subjected to a videotaped body cavity search in front of more than one hundred people, including female administrative staff.[276] "Although the Fourth Amendment does not require the complete exclusion of members of the opposite sex from areas in which searches are conducted . . . and although the security concerns articulated by prison officials are entitled to great deference," the court found that the prison administrator's statement regarding the incident was not sufficient to establish as a matter of law that the search was reasonable.[277] The court remanded for further proceedings on the inmate's Fourth Amendment claim.[278] In sum, "An individual's mere presence in a prison cell does not totally strip away every garment cloaking his Fourth Amendment rights, even though the covering that remains is but a small remnant."[279] That remnant is large enough to cover a right to private attorney-inmate communications.

C. Recognizing a Fourth Amendment Right to Private Inmate-Attorney Communications.

Under the test set out in *Hudson*, a Fourth Amendment right to privacy must be established before determining the constitutional validity of a regulation.[280] The proper inquiry is whether society is prepared to recognize a prisoner's expectation of privacy as reasonable

---

274. *Id.* The Second Circuit recently clarified that the holding in *Cohen* is limited to searches of pre-trial inmates and it refused to recognize a Fourth Amendment privacy right for convicted prisoners. Willis v. Artuz, 301 F.3d 65, 68 (2d Cir. 2002).

275. Hayes v. Marriott, 70 F.3d 1144, 1146 (10th Cir. 1995). *See generally* Mary Ann Farkas & Kathryn R. L. Rand, *Female Correctional Officers and Prisoner Privacy*, 80 MARQ. L. REV. 995 (1997); Tracy McMath, *Do Prison Inmates Retain Any Fourth Amendment Protection From Body Cavity Searches?*, 56 U. CIN. L. REV. 739 (1987); David J. Stollman, Jordan v. Gardner*: Female Prisoners' Rights to be Free from Random, Cross-Gender Clothed Body Searches*, 62 FORDHAM L. REV. 1877 (1994).

276. *Hayes*, 70 F.3d at 1147-48.

277. *Id.* at 1148. *But see* Johnson v. Phelan, 69 F.3d 144 (7th Cir. 1995), *cert. denied*, 519 U.S. 1006 (1996) (stating that prisoners retain no Fourth Amendment right of privacy while being monitored by guards while naked).

278. *Hayes*, 70 F.3d at 1148-49.

279. *Cohen*, 796 F.2d at 24.

280. *See* Hudson v. Palmer, 468 U.S. 517, 522 (1984).

when communicating with his or her attorney.[281] Because inmates have a reasonable expectation of privacy in their communications with their attorneys, and because society is prepared to recognize that expectation as reasonable, the Fourth Amendment protects the communications from unreasonable searches and seizures.[282]

Although the question has not come before the Supreme Court, many state and lower federal courts have held that the right to privacy of communications is essential to the right to effective assistance of counsel.[283] Many state regulations regarding inmate telephone calls, mail, or visits exempt communications with attorneys from the scope of authorized monitoring.[284] Moreover, under BOP regulations, prison officials may inspect and read all correspondence, unless it is labeled "special mail" (which includes attorney-client communications);[285]

---

281. *See id.* at 524-25.

282. *Contra id.* at 525-26.

283. *See supra* note 99.

284. *See, e.g.*, ALASKA STAT. § 33.30.231(c) (2002) ("A telephone call between an attorney and a prisoner . . . may not be monitored or recorded except when authorized by a court."); CAL. PENAL CODE § 636(a) (1999) ("Every person who, without permission . . . eavesdrops on or records . . . a conversation . . . between a person who is in the physical custody of a[n] . . . officer, or who is on the property of a law enforcement agency or other public agency, and that person's attorney . . . is guilty of a felony."); COLO. REV. STAT. § 16-3-403 (2002) ("Any person committed, imprisoned, or arrested . . . whether or not . . . charged with an offense [can] consult with an attorney . . . whom such person desires to see or consult, alone and in private at the place of custody, as many times and for such period each time as is reasonable."); CONN. AGENCIES REG. §§ 18-81-28, 18-81-46 (2003) (mandating that inmates be provided reasonable accommodation to make telephone calls to attorneys and that such calls not be recorded or listened to by prison staff); MASS. REGS. CODE TIT. 103, § 482.07(3)(d) (2000) ("All inmate telephone calls, except calls to pre-authorized attorney telephone numbers are subject to telephone monitoring."); MICH. COMP. LAWS ANN. § 791.270(1)(a) (1998 & Supp. 2003) (permitting the director of correctional facilities to create rules under which telephone calls may be monitored but stating that the rules "shall prescribe a procedure by which a prisoner may make telephone calls to his or her attorney . . . that are not monitored"); MINN. STAT. ANN. § 481.10 (2002) (requiring "officers or persons having in their custody a person restrained of liberty" to allow any attorney retained by or on behalf of the person restrained to conduct a private interview at the place of custody, and to provide private telephone access to such representation); OHIO REV. CODE ANN. § 2935.20 (2002) ("After the arrest, detention, or . . . other taking into custody of a person . . . such person shall be permitted . . . facilities to communicate with an attorney . . . of his choice . . . . Such person shall have a right to be visited immediately by any attorney at law so obtained . . . and to consult with him privately."); W. VA. CODE ANN. § 31-20-5e(6) (2003) ("To safeguard the sanctity of the attorney-client privilege, an adequate number of telephone lines that are not monitored shall be made available for telephone calls between inmates and their attorneys. Such calls shall not be monitored, intercepted, recorded, or disclosed in any matter."); WIS. ADMIN. CODE § DOC 309.04 (2001) (prohibiting department of corrections staff from opening or reading mail sent by an inmate to an attorney; mail received by an inmate from an attorney may only be opened by staff in the presence of the inmate).

285. 28 C.F.R. § 540.2(c) (2002).

"special mail" may only be opened and inspected for contraband in the presence of the inmate to or from whom it is sent.[286] Attorney-inmate conversations are also exempt from the routine monitoring of prisoners' telephone calls.[287] Visits by attorneys must take place in an area that allows a "degree of privacy."[288] Finally, "[s]taff may not subject visits between an attorney and an inmate to auditory supervision."[289]

While the right to confidential attorney-inmate communications is usually associated with the Sixth Amendment right to counsel, the Fourth Amendment right to privacy also merits consideration. First, the Sixth Amendment right to counsel only attaches upon the initiation of a criminal prosecution. Consequently, material witnesses, persons arrested but not formally charged, inmates whose convictions are final and whose appeals are exhausted, and other detainees who have no Sixth Amendment right but who are subject to monitoring under the expansive definition of "inmate" under § 501.3(d), would not be able to challenge the regulation on Sixth Amendment grounds.[290] Yet these persons may have as much—or greater—need to communicate in confidence with their attorneys.

The sensitive nature of the communication also makes recognition of a privacy right reasonable. Inmates have a strong interest in obtaining candid legal advice, not only regarding the circumstances that led to their imprisonment, but also respecting to personal issues that may arise while they are incarcerated;[291] they must feel free to discuss potentially embarrassing or even incriminating facts.[292] While the nature of

---

286. § 540.18(a). The regulation provides:

> [T]he Warden shall open incoming special mail only in the presence of the inmate for inspection for physical contraband and the qualification of any enclosures as special mail. The correspondence may not be read or copied if the sender is adequately identified on the envelope, and the front of the envelope is marked "Special Mail—Open only in the presence of the inmate."

Id. Additionally, "except as provided for in paragraph (c)(2) of this section [detailing screening procedures for mail sent by an inmate who the Warden has determined poses a threat to the recipient] outgoing special mail may be sealed by the inmate and is not subject to inspection." § 540.18(c)(1).

287. *See* 28 C.F.R. § 540.102 (2002) (providing that "staff may not monitor an inmate's properly placed call to an attorney. The Warden shall notify an inmate of the proper procedures to have an unmonitored telephone conversation with an attorney").

288. § 543.13(b).

289. § 543.13(e).

290. *See* § 500.1(c); Texas v. Cobb, 532 U.S. 162, 167-68 (2001) (noting that the Sixth Amendment right to counsel does not attach until after the initiation of adversary judicial proceedings, whether by formal charge, indictment, information, or arraignment).

291. For instance, an inmate may need advice regarding a divorce, attempts to terminate parental rights, real estate transactions, or immigration issues.

292. *See* Cohn, *supra* note 45, at 1254-55.

information or activities that an individual seeks to protect is not decisive in determining whether a reasonable expectation of privacy exists, the Supreme Court has indicated that it may be a factor.[293] The largely uniform case law and state and federal regulations exempting attorney-client communications from monitoring reflects recognition of the special and significant nature of these communications and the importance of confidentiality.[294] This widespread acceptance of the confidentiality of such communications demonstrates that society has long recognized the right to private attorney-inmate communications as reasonable.

Society might find the right of privacy unreasonable in the wake of recent terrorist attacks if the government demonstrated that recognizing the right presented a threat to national security. However, as discussed above, confidential communications between inmates and attorneys pose no greater risk than communications of suspected terrorists outside of the prison context. Both the Supreme Court and Congress have concluded that the threat to national security does not justify abandoning the Fourth Amendment warrant requirement.[295] Moreover, the government has not articulated any reason why obtaining a warrant before conducting the monitoring would hinder the effort to deter inmates from using attorney-client communications to further terrorist plans.[296] Because the recognition of this right does not unduly burden the government, or pose a threat to national security, society will likely continue to recognize inmates' expectation of privacy in this context as reasonable. Consequently, the Fourth Amendment proscription against unreasonable searches and seizures should apply to communications between inmates and their attorneys.[297]

---

293. *Compare* Florida v. Riley, 488 U.S. 445, 4520-52 (1989) (holding that defendant had no reasonable expectation of privacy from a helicopter legally hovering over his curtilage), *with* Dow Chemical Co. v. United States, 476 U.S. 227, 235-36 (1986). The *Dow Chemical* Court explained that the curtilage of a home receives special protection because intimate activities associated with home and the "privacies of life" take place in that area. *Id.* (quoting Oliver v. United States, 466 U.S. 170 (1984)).

294. It may also reflect the fact that many courts have held that the Sixth Amendment right to counsel requires recognition of a right to private communication with attorneys. *See supra* note 99 and accompanying text.

295. *See* discussion *supra* Part III.E.

296. *See* discussion *supra* Part III.E.

297. Congress may, of course, choose to set standards for issuing warrants in a context that differs from those set out in Title III. *See* Unites States v. United States Dist. Court (Keith), 407 U.S. 297, 322-23 (1972). *See also* discussion *supra* Part III.B.

V. 28 C.F.R. § 501.3(d) VIOLATES INMATES' FOURTH AMENDMENT RIGHTS

Recognizing a Fourth Amendment right to privacy does not automatically invalidate the monitoring regulation. The loss or curtailment of some constitutional rights is necessary to accommodate institutional security needs.[298] To that end, even regulations that violate inmates' constitutional rights will be upheld if the regulations are necessary to promote valid penological objectives.[299] Recognizing that prison administration is an "inordinately difficult" task that has been delegated to the legislative and executive branches, the Supreme Court has adopted a policy of judicial restraint and deference to prison administrators when reviewing prison regulations.[300] This policy applies equally to convicted inmates and pretrial detainees.[301]

Given the tension between inmates' constitutional rights and the institutional needs of prison facilities (including the paramount goal of internal security), courts struggled to find a standard of review for prison regulations that struck the appropriate balance. In *Procunier v. Martinez*,[302] the Supreme Court reviewed mail censorship regulations.[303] The Court held that the regulations should be upheld if they furthered an important or substantial governmental interest unrelated to the suppression of expression, and if the constitutional infringement was no greater than necessary to protect that interest.[304] After *Martinez*, the Supreme Court decided *Pell v. Procunier*,[305] *Jones v. N.C. Prisoners'*

---

298. Hudson v. Palmer, 468 U.S. 517, 524 (1984). Internal security is only one of the objectives of restrictions on inmate rights. In addition, "[t]hese restrictions . . . also serve, incidentally, as reminders that, under our system of justice, deterrence and retribution are factors in addition to correction." *Id.*

299. Turner v. Safley, 482 U.S. 78, 89 (1987).

300. *Id.* at 84-85.

301. Bell v. Wolfish, 441 U.S. 520, 546 (1979) (stating, in general, "[a] [pretrial] detainee simply does not possess the full range of freedoms of an unincarcerated individual."). *Id.* The Court noted:

> There is no basis for concluding that pretrial detainees pose any lesser security risk than convicted inmates. Indeed, it may be that in certain circumstances they present a greater risk to jail security and order. In the federal system, a detainee is committed to the detention facility only because no other less drastic means can reasonably assure his presence at trial. As a result, those who are detained prior to trial may in many cases be individuals who are charged with serious crimes or who have prior records.

Id. at 546 & n.28 (internal citations omitted).

302. 416 U.S. 396 (1974).

303. *Id.* at 398-99.

304. *Id.* at 413.

305. 417 U.S. 817 (1974).

Labor Union, Inc.,[306] *Bell v. Wolfish*,[307] and *Block v. Rutherford*.[308] In each of these cases, the Supreme Court abandoned the standard used in *Martinez* and instead inquired whether the challenged prison regulations were reasonably related to legitimate penological objectives. In *Turner v. Safley*,[309] the Court resolved the confusion regarding the standard of review in prison regulation cases: "If *Pell*, *Jones*, and *Bell* have not already resolved the question posed in *Martinez*, we resolve it now: when a prison regulation impinges on inmates' constitutional rights, the regulation is valid if it is reasonably related to legitimate penological interests."[310]

The Supreme Court then set out the factors that courts should consider when evaluating the reasonableness of a particular regulation: (1) there must be a rational relationship between the regulation and the penological interest; (2) the court must consider whether there are alternative means of exercising the right that are available to inmates; (3) it must consider the impact that accommodation of the asserted constitutional right would have on prison officials, other inmates, and prison resources; and (4) the absence of ready alternatives is to be regarded as evidence of the reasonableness of the regulation (while the existence of obvious, easy alternatives may provide evidence of the regulation's unreasonableness).[311] Thus, challenging the monitoring regulation on Fourth Amendment grounds is a two-step process. The regulation must be shown to violate an inmate's Fourth Amendment rights. Even if this burden is met, the court must then determine whether that regulation is nevertheless reasonably related to a legitimate penological interest. If it is, it will be sustained. Otherwise, it must be struck down.[312]

A. Warrantless Monitoring Authorized by § 501.3(d) Violates Inmates' Fourth Amendment Rights.

One can argue that, although the Fourth Amendment protects inmates' justifiable expectation of privacy in their communications with their attorneys, the Fourth Amendment does not require a warrant before monitoring can occur. Indeed, the pre-*Hudson* cases accepted

306. 433 U.S. 119 (1977).

307. 441 U.S. 520 (1979).

308. 468 U.S. 576 (1984).

309. 482 U.S. 78, 89-90 (1987).

310. *Id.* at 89.

311. *Id.* at 89-91. *See also* Overton v. Bazzetta, 123 S. Ct. 2162, 2167-70 (2003) (applying the *Turner* standard of review and analyzing the four *Turner* factors to prison regulation that restricted visitation by children).

312. *Turner*, 482 U.S. at 89.

this argument in the case of cell searches,[313] and concluded that searches merely had to be reasonable.[314] In *Keith,* the Supreme Court held that the Executive was bound by the Fourth Amendment when conducting national security surveillance of domestic targets, but noted exceptions to the warrant requirement.[315] The monitoring regulation, however, does not fall into any of those "carefully delineated exceptions."[316]

Departure from the Fourth Amendment's warrant requirement in the present situation is not justified.[317] While the need for prison security may make warrantless searches of prison cells reasonable, no comparable concerns are raised by confidential inmate-attorney communications. And, as the Supreme Court explained in *Keith*, national security concerns do not automatically justify dispensing with the warrant requirement.[318]

---

313. *See, e.g.*, United States v. Chamorro, 687 F.2d 1, 4 (1st Cir. 1982) ("We expressly reject appellant's contention that . . . a warrant was required."); United States v. Lilly, 576 F.2d 1240, 1244 (5th Cir. 1978) ("The government needs neither a warrant nor probable cause to conduct a search or seizure in the prison context because of prisoners' decreased expectations of privacy and because of the exigencies inherent in the prison environment."); United States v. Stumes, 549 F.2d 831, 832 (8th Cir. 1977) (noting that obviation of the warrant requirement in prisons rests in part on diminished expectations of privacy).

314. *See, e.g.*, *Chamorro*, 687 F.2d at 4-5; *Lilly*, 576 F.2d at 1244-45; *Stumes*, 549 F.2d at 832.

315. United States v. United States Dist. Court (Keith), 407 U.S. 297, 318-21 (1972).

316. *Id.* at 318 (noting that the exceptions to the warrant requirement generally "serve to the legitimate needs of law enforcement officers to protect their own well-being and preserve evidence from destruction"). Section 501.3(d) is not designed to protect law enforcement offices or preserve evidence. Nor does the regulation fall into the category of "special needs" exceptions to the warrant requirement. The Supreme Court has recognized that "in limited circumstances a search unsupported by either warrant or probable cause can be constitutional when 'special needs' *other than the normal need for law enforcement* provide sufficient justification." Ferguson v. City of Charleston, 532 U.S. 67, 76 n.1 (2001) (emphasis added). The Court has approved "special needs" searches when the privacy interests at issue are minimal and exceptional circumstances make the probable cause and warrant requirement impracticable. *Id.* at 76, 78; Skinner v. Railway Labor Execs. Ass'n, 489 U.S. 602, 624 (1989). Section 501.3(d) implicates significant privacy interests and serves a general law enforcement purpose. Moreover, obtaining a warrant for monitoring is not impracticable. For these reasons, 501.3(d) does not meet the criteria for the special needs exception to the warrant requirement. *See Ferguson*, 532 U.S. at 78, 81 (refusing to apply special needs exception when the invasion of privacy was substantial and law enforcement was a central purpose of the searches at issue).

317. *See supra* Part III.B.

318. *Keith*, 407 U.S. at 320. *See also supra* Part III.B. The Court's holding in *Keith* was limited to domestic threats to national security, but the same arguments could apply to foreign threats. National security concerns may, however, justify procedures for issuing a warrant for prison monitoring that vary from those set out in Title III, FED. R. CRIM. P. 41, or FISA. The *Keith* Court acknowledged that security surveillance may involve different policy and practical considerations than those involved in surveillance of other "ordinary crimes." *Keith*, 407 U.S. at 322-23. Those considerations may justify different

On the other hand, prior judicial approval and ongoing judicial review are necesary to ensure against violations of the attorney-client privilege. Once an inmate recveives notification that all communications with his or her attorney may be monitored, the inmate has no means of challenging the decision.[319] For this reason, merely giving notice that monitoring will occur does not make the search and seizure reasonable. Knowing that your rights are being violated is of no comfort if you are without the means to end or even challenge the violation.

Moreover, while the regulation refers to procedures designed to safeguard the privilege, the BOP Director retains discretion over the precise procedures to be implemented.[320] Neither the inmate nor his or her attorney has a right under the regulation to know what procedures are being employed or to challenge the sufficiency of the procedures.[321] Furthermore, even if the procedures are acceptable, without judicial oversight an inmate or attorney cannot know whether the prison officials are following procedures. Finally, the federal officers involved in the monitoring make the final decision as to whether a communication is privileged.[322] Making such a determination is likely to be a complex matter, particularly if the government suspects that the inmate is speaking in code or passing hidden messages in otherwise innocuous conversations.

Weighed against the substantial intrusion upon inmates' rights, the warrant requirement is a minor hurdle for the Attorney General. Given the highly sensitive nature of the communications, and the inherent problems noted above in having all decisions made by the Executive Branch, requiring federal officials to obtain a warrant before monitoring attorney-inmate communications is necessary to make any search or seizure of attorney-inmate communications reasonable. Because § 501.3(d) does not require a warrant or allow for any judicial involvement or review, it violates the Fourth Amendment.

---

warrant standards, so long as the standards are reasonable. *Id.* at 322-24. A key feature of any reasonable procedure must be prior judicial review.

319. The Attorney General's determination that the "reasonable suspicion" standard has been met is final. *See* 28 C.F.R. § 501.3(d) (2002).

320. § 501.3(d)(3). This section states:

> The Director, Bureau of Prisons, with the approval of the Assistant Attorney General for the Criminal Division, shall employ *appropriate* procedures to ensure that all attorney-client communications are reviewed for privilege claims and that any properly privileged materials (including, but not limited to, recordings of privileged conversations) are not retained during the course of the monitoring.

Id. (emphasis added).

321. *See id.*

322. *Id.*

B. Applying the Turner *Factors*

Generally, even a prison regulation that impinges on a prisoner's constitutional rights is still valid if it is reasonably related to a legitimate penological interest.[323] An examination of § 501.3(d) in light of the four *Turner* factors makes it clear that the regulation is unreasonable and invalid.

1. Valid, Rational Connection

A prison regulation cannot stand if "the logical connection between the regulation and the asserted goal is so remote as to render the policy arbitrary or irrational."[324] Deterring future acts of terrorism is not a *penological* objective. Thus, to the extent that a penological objective is required—typically related to institutional security—this factor weighs against upholding the regulation.[325] Because it does not contain a penoloical objective, the regulation should not be upheld.

However, the test is often phrased as requiring a rational connection between the prison regulation and a legitimate *governmental* interest.[326] Deterrence of crime is certainly a legitimate governmental interest. Although doubtful that monitoring every conversation between a prisoner and his or her attorney would effectively deter the most determined terrorist from passing coded messages, a rational connection between the regulation and the goal of deterrence probably exists. If rational relation to a *governmental* interest is sufficient to satisfy this factor, then it will weigh in favor of upholding the regulation.

2. Alternative Means

If inmates have other means of exercising the asserted right—here, the right to communicate privately with attorneys—then judicial deference to the rule-making of prison officials is appropriate.[327] Obviously,

---

323. Shaw v. Murphy, 532 U.S. 223, 229 (2001) (noting that in *Turner*, the Court adopted "a unitary, deferential standard for reviewing prisoner constitutional claims: '[W]hen a prison regulation impinges on inmates' constitutional rights, the regulation is valid if it is reasonably related to legitimate penological interests.'") (quoting *Turner*, 482 U.S. at 89).

324. *Id.* at 89-90. *See also Shaw*, 532 U.S. at 229-230. Specifically, the regulation itself states that communications will be monitored "for the purpose of deterring future acts that could result in death or serious bodily injury to persons, or substantial damage to property that would entail the risk of death or serious bodily injury to persons." *Id.* The Court determined that "[i]f the connection between the regulation and the asserted goal is 'arbitrary or irrational,' then the regulation fails, irrespective of whether the other factors tilt in its favor." *Id.* (quoting *Turner*, 482 U.S. at 89-90).

325. 28 C.F.R. § 501.3(d) (2002).

326. *Turner*, 482 U.S. at 89-90.

327. *Id.*

inmates have very limited avenues of communicating with anyone outside of the prison, including their attorneys. Moreover, on its face, the regulation applies to any attorney with whom the prisoner communicates.[328] Section 501.3(d) also allows the government to monitor every available means of communication,[329] leaving inmates with no means of communicating privately with legal counsel, even though confidential communication is an essential component of a prisoner's right to effective assistance of counsel.[330] Thus, this factor clearly weighs against upholding § 501.3(d).

3. Impact of Exercised Right

Courts are sensitive to the fact that the exercise of certain rights within the closed prison environment may have a "ripple effect" on other inmates and staff.[331] However, accommodating inmates' right to confidential communications with their attorneys will have little, if any, impact on the prison environment. Current regulations—aside from § 501.3(d)—protect the confidentiality of such communications, and prison officials should already have procedures in place to protect the confidentiality of communications while simultaneously ensuring internal security.[332] These security procedures will remain in place even if § 501.3(d) is upheld because the vast majority of inmates will not be subject to monitoring.

While the inmates who are identified as potential threats (as defined in § 501.3(d)) may pose a higher risk to prison security in general, warrantless monitoring of their communications with their attorneys is not likely to significantly reduce the internal threat. Moreover, assuming a warrant is obtained, the monitoring can still take place. Therefore, allowing those inmates to exercise their right to confidential communication with counsel does not result in significantly less liberty or safety for others in the prison.

4. Alternatives

The existence of obvious, easy alternatives for achieving the same objective is strong evidence that the regulation is unreasonable.[333] While

328. *See* § 501.3(d).

329. *See id.*

330. *See supra* note 99.

331. *Id.*

332. *See* §§ 543.13(b), 543.13(e), 540.18(a), 540.18(c)(1), 540.102 (addressing respectively, the time and place of attorneys' visits, permissible recordings of attorneys' visits, opening special mail, sealing special mail, and the monitoring of inmate phone calls).

333. *Id.*

prison officials are not obligated to find the least restrictive means of accommodating inmates' constitutional rights, a court may find that the regulation does not meet the reasonable relationship standard if an alternative exists that fully accommodates those rights at minimal cost to valid penological interests.[334]

Section 501.3(d) represents an exaggerated and unreasonable response to the government's concerns. Title III, FED. R. CRIM. P. 41, and FISA are easy, obvious alternatives that are available at minimal cost to penological interests. Requiring the Executive branch to seek a warrant before monitoring communications between inmates and attorneys does not impose any greater burden on prison officials, and only imposes a minimal burden on the Attorney General.[335] This final factor, then, also weighs against upholding § 501.3(d).[336]

VI. CONCLUSION

Weighing the four relevant factors, clearly the monitoring regulation does not pass constitutional muster and should be struck down. In a time of increasing suspicion and fear, it is the responsibility of the executive branch to instill confidence in our system of government, including the legislative and judicial branches. By choosing to ignore statutes enacted by Congress for conducting surveillance and bypassing prior judicial review, the Attorney General instead breeds distrust.

Section 501.3(d) is also unnecessary and unconstitutional. Existing statutes and rules allow the Attorney General to monitor inmate-attorney communications after obtaining a warrant.[337] Dispensing with the warrant requirement, as § 501.3(d) purports to do, violates the right to confidential communications between the inmates and their attorneys—a right that society is prepared to recognize as reasonable and which therefore, receives protection under the Fourth Amendment. For these reasons, the regulation should be struck down.

---

334. *Id.* at 90-91.

335. *See supra* Part II.D.

336. *See Turner*, 482 U.S. at 97-98 (striking down regulation prohibiting inmates from marrying without the permission of the superintendent of the prison because, among other reasons, it was an exaggerated response to the stated security goal, and obvious, easy alternatives existed that would "accommodate the right to marry while imposing a *de minimis* burden on the pursuit of security objectives").

337. *See supra* Part II.