COERCING CLIENTS: CAN LAWYER GATEKEEPER RULES WORK?

Fred C. Zacharias

[pages 455–504]

Abstract: Recent federal regulations and amendments to the Model Rules of Professional Conduct—most of which have responded to lawyer involvement in corporate scandals—rest on the assumption that lawyers have a role to play in forcing clients to act legally, morally, or appropriately. Lawyers are distinctive, perhaps even unique among professionals, in that they are sometimes legally authorized to force clients into obeying the lawyers’ advice. This Article reviews the rules that empower lawyers in this way, with a focus on the corporate context. For the most part, the recent regulatory changes take a static view of the lawyer-client relationship. They assume that if lawyers are authorized or required to counteract proposed client misconduct, lawyers will do so and less client misconduct will result. This Article demonstrates that the reality is far more complex. Lawyers and clients have incentives to implement coercive rules in ways that serve reasons wholly unrelated to the rules’ purposes. Code drafters and those evaluating lawyers’ coercive authority, therefore, must confront the fact that attorney-client relationships are dynamic—that is, that a change in the power of one party in the relationship has ripple effects. This practical reality influences both the positions of lawyers in deciding whether to favor or oppose particular regulation and the likely effectiveness of coercive rules.
Abstract: Information to, from, and about U.S. persons routinely comes into the possession of the National Security Agency (the “NSA”) through the lawful warrantless surveillance of foreign persons abroad. The NSA’s internal administrative guidelines allow such information to be disseminated to law enforcement if it evinces any criminal conduct on the part of the U.S. person. This information may therefore be used to initiate domestic criminal investigations against U.S. citizens and other protected persons despite the fact that no warrant authorized the initial surveillance. The NSA’s guidelines contain no qualification as to the type of criminal offense that may be revealed, and no consideration of the individual’s reasonable expectation of privacy. Using encrypted Internet telephony as an example, this Article proposes a change to the NSA’s internal guidelines that would prevent dissemination of information gained through the frustration of the reasonable privacy expectations of protected persons unless exigent circumstances or serious threats to national security were presented.

NOTES

OLD RULE, NEW THEORY: REVISING THE PERSONAL BENEFIT REQUIREMENT FOR TIPPER/TIPPEE LIABILITY UNDER THE MISAPPROPRIATION THEORY OF INSIDER TRADING

Abstract: Under the classical theory of insider trading, tipper/tippee liability may arise only when the tipper makes the relevant disclosure to obtain a personal benefit. Courts are divided, however, as to whether this personal benefit requirement applies to the misappropriation theory of insider trading. This Note argues that because the personal benefit requirement is severely flawed, courts should not impose it in misappropriation
cases. Instead, courts adjudicating misappropriation cases should require that (1) the tipper was at least reckless as to whether he or she would either benefit personally or harm the information source by tipping, and (2) the tipper was at least reckless as to whether someone in the line of tippees would use the information to trade. This standard should be subject only to the tipper’s defense that the disclosure was made in a good faith attempt to prevent criminal activity reasonably certain to cause substantial physical or financial harm to others.

TERRORIZING JUSTICE: AN ARGUMENT THAT PLEA BARGAINS STRUCK UNDER THE THREAT OF “ENEMY COMBATANT” DETENTION VIOLATE THE RIGHT TO DUE PROCESS

Carl Takei

[pages 581–626]

Abstract: As part of the War on Terror, the President has detained certain individuals as “enemy combatants”—a form of military detention that is preventive, non-criminal, and of indefinite duration. Some terrorism defendants appear to have pled guilty to criminal charges in order to avoid being detained as enemy combatants. This Note argues that plea bargains induced by threats of enemy combatant detention do not arise from the normal give-and-take of plea bargaining, create serious public policy concerns, and serve no societal interests that could not be served equally well by other means. It therefore concludes that the courts should hold such plea bargains per se unenforceable under the Due Process Clause of the Fifth Amendment.

CONFIDENTIAL INFORMANTS IN NATIONAL SECURITY INVESTIGATIONS

Daniel Ward

[pages 627–658]

Abstract: Although a body of law has developed around the use of confidential informants in criminal investigations, the role of informants in national security matters is less clearly defined. This Note first examines the limitations on the use of informants in the criminal context that are imposed by the Fourth Amendment, a detailed set of guidelines issued by the Attorney General, and other sources of law. It then turns to the treatment of infor-
mants by the major sources of national security law, including the Foreign Intelligence Surveillance Act. Ultimately, this Note concludes that in the national security context, government agents are free from many of the restrictions placed on the use of informants in criminal investigations. Although this relative freedom may be necessary given the immediate challenge of combating international terrorism, care should be taken that the executive branch does not use informants in a way that violates individual privacy or oversteps other proper investigative boundaries.
COERCING CLIENTS: CAN LAWYER GATEKEEPER RULES WORK?

Fred C. Zacharias*

Abstract: Recent federal regulations and amendments to the Model Rules of Professional Conduct—most of which have responded to lawyer involvement in corporate scandals—rest on the assumption that lawyers have a role to play in forcing clients to act legally, morally, or appropriately. Lawyers are distinctive, perhaps even unique among professionals, in that they are sometimes legally authorized to force clients into obeying the lawyers’ advice. This Article reviews the rules that empower lawyers in this way, with a focus on the corporate context.

For the most part, the recent regulatory changes take a static view of the lawyer-client relationship. They assume that if lawyers are authorized or required to counteract proposed client misconduct, lawyers will do so and less client misconduct will result. This Article demonstrates that the reality is far more complex. Lawyers and clients have incentives to implement coercive rules in ways that serve reasons wholly unrelated to the rules’ purposes. Code drafters and those evaluating lawyers’ coercive authority, therefore, must confront the fact that attorney-client relationships are dynamic—that is, that a change in the power of one party in the relationship has ripple effects. This practical reality influences both the positions of lawyers in deciding whether to favor or oppose particular regulation and the likely effectiveness of coercive rules.

INTRODUCTION

The allocation of power in the attorney-client relationship is distinctive. Like most service providers, lawyers are employees, agents, or independent contractors. They typically must do their clients’ bidding.1 Like other professionals, lawyers also have special expertise

* Herzog Endowed Research Professor, University of San Diego School of Law. The Author thanks Professors Bruce Green, Shaun Martin, and David McGowan for their thoughtful comments on earlier drafts of this Article; Siraj Bayaan, Brian Katusian, and Ryan Keller for their research assistance; and the University of San Diego School of Law for its generous research support.

1 See, e.g., MODEL RULES OF PROF’L CONDUCT R. 1.2(a) (2002) (stating that “a lawyer shall abide by a client’s decisions concerning the objectives of representation and . . . shall consult with the client as to the means by which they are to be pursued”); MODEL RULES OF
that often leads clients to defer to their recommendations. Lawyers, however, are unusual in the degree of control they exercise within the relationship. Unlike in medical decision making, for example, some legal decisions are for lawyers, and lawyers alone, to make. Other professionals may be able to influence those who hire them, but lawyers have legally recognized authority to pressure clients into accepting their advice—particularly when that advice concerns illegal or wrongful conduct.

I do not mean to overstate the case. Lawyers do not always have coercive authority. Nor do the professional codes explicitly sanction pressure on clients. Nevertheless, the codes do envision lawyers using their position to persuade, and sometimes force, clients to act in accordance with the lawyers’ view of appropriate conduct. In other instances, the codes simply give lawyers authority to override clients’ commands.

Lawyers can exercise coercive power in a variety of ways. They may threaten to resign when clients do not conform to their advice. Lawyers may insist upon particular legal tactics. And, through the coercive mechanism that is most commonly discussed in the literature, lawyers sometimes have the right to reveal otherwise confidential information about the client. Threatening a revelation typically forces the client to act as the lawyer wishes.

**PROF’L CONDUCT R. 1.2(a) (1983) (same); MODEL CODE OF PROF’L RESPONSIBILITY EC 7-7 (1969) (noting that “the authority to make decisions is exclusively that of the client”); cf. MODEL RULES OF PROF’L CONDUCT R. 1.2 cmt. (2002) (clarifying that “this Rule does not prescribe how . . . disagreements [about the means] are to be resolved”).**

2 See MODEL RULES OF PROF’L CONDUCT R. 1.2 cmt. (2002) (stating that “[c]lients normally defer to the special knowledge and skill of their lawyer with respect to the means to be used to accomplish their objectives”).

3 See MODEL RULES OF PROF’L CONDUCT R. 1.2 cmt. (1983) (stating “a lawyer is not required to pursue objectives or employ means simply because a client may wish that the lawyer do so”).

4 See MODEL RULES OF PROF’L CONDUCT R. 2.1 (2002) (allowing lawyers to advise clients concerning the moral and political ramifications of their conduct); see also Upjohn Co. v. United States, 449 U.S. 383, 392 (1981) (characterizing promoting clients’ “compliance with the law” as one of the key justifications for giving lawyers the ability to obtain privileged information from clients); Fred C. Zacharias, Rethinking Confidentiality, 74 IOWA L. REV. 351, 369 (1989) (describing the law compliance rationale for attorney-client confidentiality).

5 See infra notes 29–42 and accompanying text.

Consider this ability of lawyers to use confidences to pressure clients. Legal ethics codes always have made some provision for disclosure,7 Spurred by public reaction to lawyer involvement in recent corporate scandals,8 the American Bar Association (the “ABA”) adopted amendments to the Model Rules of Professional Conduct in 2002 and 2003 that make explicit an expanded right of attorneys, especially corporate attorneys, to reveal or threaten to reveal information.9 Ad-

---

7 E.g., Model Rules of Prof’l Conduct R. 1.6(b) (2002); Model Rules of Prof’l Conduct R. 1.6(b) (1983); Model Code of Prof’l Responsibility DR 4-101(C) (1969).


9 See Model Rules of Prof’l Conduct R. 1.6(b), 1.13(b) (2002). The revised Model Rule 1.6(b) provides, in pertinent part:

(b) A lawyer may reveal information relating to the representation of a client to the extent the lawyer reasonably believes necessary:

(1) to prevent reasonably certain death or substantial bodily harm;
(2) to prevent the client from committing a crime or fraud that is reasonably certain to result in substantial injury to the financial interests or property of another and in furtherance of which the client has used or is using the lawyer’s services;
(3) to prevent, mitigate or rectify substantial injury to the financial interests or property of another that is reasonably certain to result or has resulted from the client’s commission of a crime or fraud in furtherance of which the client has used the lawyer’s services . . . .

Model Rules of Prof’l Conduct R. 1.6(b) (2002). The revised Model Rule 1.13 provides, in pertinent part:

(b) If a lawyer for an organization knows that an officer, employee or other person associated with the organization is engaged in action, intends to act or refuses to act in a matter related to the representation that is a violation of a legal obligation to the organization, or a violation of law that reasonably might be imputed to the organization, and that is likely to result in substantial injury to the organization, then the lawyer shall proceed as is reasonably necessary in the best interest of the organization. Unless the lawyer reasonably believes that it is not necessary in the best interest of the organization to do so, the lawyer shall refer the matter to higher authority in the organization, including, if warranted by the circumstances to the highest authority that can act on behalf of the organization as determined by applicable law.

(c) Except as provided in Paragraph (d), if

(1) despite the lawyer’s efforts in accordance with paragraph (b) the highest authority that can act on behalf of the organization insists upon or
ministrative regulations implementing the federal Sarbanes-Oxley Act render mandatory some attorney disclosures of corporate misconduct.\textsuperscript{10} Pending regulations propose additional requirements.\textsuperscript{11} One interpretation of these provisions is that society expects lawyers to reveal corporate clients’ misconduct on a routine basis.\textsuperscript{12} A second interpretation is that the ability to disclose should only be exercised rarely, but that a disclosure rule provides lawyers with a tool they can use to persuade clients to act properly.\textsuperscript{13} Strict proponents of attorney-client confidentiality characterize the process by which lawyers force clients to amend their conduct at pain of exposure as a fails to address in a timely and appropriate manner an action, or a refusal to act, that is clearly a violation of law, and (2) the lawyer reasonably believes that the violation is reasonably certain to result in substantial injury to the organization, then the lawyer may reveal information relating to the representation whether or not Rule 1.6 permits such disclosure, but only if and to the extent the lawyer reasonably believes necessary to prevent substantial injury to the organization.

\textbf{Model Rules of Prof’l Conduct R. 1.13 (2002).} \textsuperscript{10} See 17 C.F.R. § 205.3(b) (2005). Under this provision, lawyers who become aware that a material violation of securities law or breach of fiduciary duty or similar violation by the company or any agent thereof is reasonably likely must notify the chief executive officer or chief legal officer. If the attorney does not obtain an appropriate response, the attorney must report the violation to an audit committee or the board of directors. At this stage, a failure of the highest authority to correct a violative securities filing only triggers permissive authority to disclose the violation to the SEC. \textit{Id.} § 205.3(d)(2).


form of extortion that undermines the very notion of an attorney-client trust relationship.\textsuperscript{14}

For the most part, that is as far as the analysis has proceeded. Proponents argue that allowing or requiring lawyers to disclose future client misconduct benefits society and lawyers’ ability to act as moral individuals,\textsuperscript{15} while opponents argue that it undermines the adversary system and client autonomy.\textsuperscript{16} Commentators treat the issue as a static question of whose interests should control.

This Article suggests that disclosure exceptions, as well as other professional regulations that enable lawyers to coerce clients into acting “appropriately,” need to be analyzed in greater depth.\textsuperscript{17} The prac-
ticalities of attorney-client relationships cannot be reduced to a single paradigm. As professional rules enhance lawyers’ power over clients, clients are given reasons to distance themselves from lawyers. Lawyers, in turn, may enjoy their increased status, but may prefer to work to maintain or regain the previous relationship.

Changes in the rules thus have a dynamic, rather than a static, effect. Systemically, according lawyers coercive power may be designed to produce one consequence (for example, the public revelation of client misconduct), but in the long run may achieve different (and perhaps counter-productive) consequences for lawyers, clients, and society by changing the interplay of the participants in the attorney-client relationship. On an individual basis, lawyers’ personal incentives will affect how they use the power that the rules give them. Whether and how lawyers exercise coercive power probably depends on context far more than participants in the debates thus far have acknowledged.

This Article attempts to further the discussion by scrutinizing the process of lawyer coercion—including what might loosely be termed “attorney blackmail”—and considering its likely effects on lawyers and clients. Threats of disclosure, resignation, or other consequences clients consider unpleasant usually do not constitute blackmail in the strict legal sense. Because the lawyer who coerces a client ordinarily does not obtain personal benefits when the client submits, and because the lawyer typically demands a client response that the lawyer (or society) has a right to expect or that the lawyer has a right to psychological, relational, and status concerns or nuances in how different lawyers and clients will respond to variations in the rules. Id. at 1827–33.

18 Under the Model Penal Code, the crime of blackmail is a form of theft, and is limited to situations in which the blackmailer “obtains property of another” by the use of a threat of disclosure. Model Penal Code § 223.4 (1980); see, e.g., N.H. Rev. Stat. Ann. § 637:1 (1955) (noting that theft represents a single offense and incorporates blackmail); Utah Code Ann. § 76-6-403 (1953) (stating that blackmail is a form of theft); Rael v. Sullivan, 918 F.2d 874, 876 n.1 (10th Cir. 1990) (quoting 31A Am. Jur. 2d Extortion § 49 as stating: “Under the common law and most recent statutory codes and proposals, extortion by a private person, or blackmail, is limited to obtaining property . . . .”); State v. Talley, 466 A.2d 78, 81 (N.J. 1983) (referencing the Model Penal Code and noting theft crimes that involve the involuntary transfer of property). A definition limiting the blackmailer’s potential benefit to “property,” however, may be too constrained. See, e.g., WAYNE R. LAFAYE, Criminal Law § 20.4(a), at 1014 (4th ed. 2003) (noting broader statutes that encompass “pecuniary advantage” or “anything of value” or the like” or “any act against [the victim’s] will”); Leo Katz, Blackmail and Other Forms of Arm-Twisting, 141 U. Pa. L. Rev. 1567, 1568 (1993) (noting that “[i]t is also easy, but also wrong, to think that blackmail is essentially a property crime” and providing counter-examples).

19 The issue of whether it is improper for a “blackmailer” to extort a socially beneficial result—even legally required conduct—is complex. See, e.g., LAFAYE, supra note 18.
produce herself, the lawyer’s threats may not be subject to criminal prosecution. Nevertheless, this Article refers to such coercion as “attorney blackmail” and rules that authorize coercion as “blackmail rules” because those terms best encapsulate the process envisioned by the rules: lawyers are given (and sometimes exercise) power to coerce an involuntary surrender of clients’ traditional authority to dictate terms and control the subject of representation.

Part I identifies the ways in which lawyer coercion may occur in the corporate context. Part II considers when corporate lawyers would (or would not) want the ability to force clients to change their behavior and lawyers’ incentives (and disincentives) to implement the option of making coercive threats. Part III notes the ramifications of these countervailing considerations for the conduct of lawyers and clients, particularly corporate clients.

Part IV demonstrates that, to the extent it is in society’s interest to authorize or require attorneys to pressure clients under some cir-

---

§ 20.4(a), at 1015–16 (discussing cases and statutes suggesting that an “intent to gain” is not always a requirement of blackmail); Mitchell N. Berman, The Evidentiary Theory of Blackmail: Taking Motives Seriously, 65 U. CHI. L. REV. 795, 864–65 (1998) (discussing the issue of “whether blackmail should be criminalized when the blackmailer’s ostensible objective is a public, rather than private, good”); Jennifer Gerarda Brown, Blackmail as Private Justice, 141 U. PA. L. REV. 1935, 1936 (1993) (arguing that blackmail based on incriminating information is “potentially paradoxical because it might confer social benefits not produced by other kinds of blackmail”); Russell Hardin, Blackmailing for Mutual Good, 141 U. PA. L. REV. 1787, 1790–92 (1993) (analyzing the argument that plea bargaining and other forms of coercion designed to extract a good result are ordinary, or morally justified, blackmail).

20 One example of this occurs when a lawyer forces the client to reveal wrongdoing that the lawyer has a legal right to reveal herself. See Scott Altman, A Patchwork Theory of Blackmail, 141 U. PA. L. REV. 1639, 1639 n.2 (1993) (discussing, inter alia, why it is wrong to place a condition on doing an optional act); Berman, supra note 19, at 796 (analyzing the “so-called paradox of blackmail” that offering to refrain from revealing embarrassing information that one has a right to reveal (or not reveal) may become unlawful if offered in exchange for payment); Wendy J. Gordon, Truth and Consequences: The Force of Blackmail’s Central Case, 141 U. PA. L. REV. 1741, 1743 (1993) (justifying blackmail law in “paradox” cases on the basis that “people do not invariably have a right to threaten to do or not do the things they are at liberty to do or not do”); Katz, supra note 18, at 1568 (discussing examples in which legal objectives may become illegal when offered in exchanged for money); James Lindgren, Unraveling the Paradox of Blackmail, 84 COLUM. L. REV. 570, 670–71 (1984) (highlighting the complexity of the paradox).

21 Cf. Peter J. Henning, Sarbanes-Oxley Act § 307 and Corporate Counsel: Who Better to Prevent Corporate Crime?, 8 BUFF. CRIM. L. REV. 323, 328 (2004) (stating that a mandatory withdrawal rule may enable lawyers to “use the withdrawal requirement strategically to force the corporation to accede to the lawyer’s demand, i.e., blackmail”).

22 See infra notes 29–42 and accompanying text.

23 See infra notes 43–68 and accompanying text.

24 See infra notes 69–110 and accompanying text.
cumstances, that conclusion results from a balance of competing factors. The professional rules, however, tend to rely on shorthand methods to implement the balance. Corporations and lawyers may favor or oppose rules supporting coercion for reasons relating to their personal incentives, having nothing whatsoever to do with the valid concerns underlying the rules. Lawyers also may implement the rules in ways that undermine the achievement of the rulemakers’ goals.

The Article’s analysis therefore helps explain why segments of the bar take certain positions in the debates concerning, for example, rules allowing disclosure or threatening disclosure of confidential information. Understanding the personal costs and benefits of coercive authority to attorneys informs the objective analysis of when society should wish to authorize attorney blackmail. Recognizing that the effects of granting coercive authority are dynamic also may help determine whether blackmail provisions should take permissive or mandatory forms. It may enable rulemakers to craft the provisions in ways that best provide incentives for appropriate long-term attorney conduct.

This Article is concerned with all forms of attorney coercion and all contexts in which it occurs. But because most of the recent regulatory developments have focused on issues relating in some way to the revelation of client information—for example, confidentiality exceptions or reporting requirements—and have involved the corporate context, this Article does so as well. The main body of this Article limits itself to situations in which in-house or external corporate counsel might be inclined to threaten action if her client does not reconsider proposed conduct.

The situation of criminal defendants raises distinct issues, as does the circumstance in which lawyers develop close trust relationships with individual, sometimes unsophisticated, clients. Therefore, this

25 See infra notes 111–138 and accompanying text.
26 To avoid confusion, this Article will refer to lawyers as female and other actors as male.
27 Criminal defendants may have special constitutional rights that encompass more of a right to be free from lawyer blackmail. See Whiteside v. Scurr, 744 F.2d 1323, 1328 (8th Cir. 1984) (holding that a lawyer’s threat to impeach a client if he perjured himself undermined the attorney-client trust relationship and therefore constituted ineffective assistance of counsel), rev’d sub nom. Nix v. Whiteside, 475 U.S. 157 (1986). As a theoretical matter, because of the threatening context in which criminal representation occurs, there may be special reason to assure criminal clients counsel who are independent of the state. Arguably, many of the same justifications apply to other clients who are especially dependent on their lawyers or unable to navigate the legal system without their direction. See Simon, supra note 15, at 170–94 (analyzing the question “Is Criminal Defense Different?”); Fred C. Zacharias, The Civil-Criminal Distinction in Professional Responsibility, 7 J. CONTEM.
Article initially sets those contexts to the side. Part V, however, offers some thoughts about the degree to which this Article’s analysis applies to non-corporate settings and to different techniques of lawyer coercion.28

I. ATTORNEY COERCION IN THE CORPORATE CONTEXT

Rules governing corporate lawyers’ obligations typically refer to their targets as lawyers representing an organization.29 By their terms, the rules apply equally to in-house and external counsel. The incentives of the various corporate lawyers implementing the rules often differ, however, as do the methods by which they can (or are expected to) influence corporate conduct.

Corporate attorneys come in many different forms. In-house counsel ordinarily are salaried employees and have the organization as their sole client. In-house counsel may themselves be officers or supervisory personnel (for example, the general counsel), or they may be lower-level staff. The functions of some in-house counsel are limited to addressing legal issues. Other in-house lawyers perform dual “legal” and “business” roles.

In contrast, external counsel typically confine their activities to legal representation. They may have multiple clients, corporate or otherwise. The client organization in question may constitute large or small portions of their practice.

When a corporate attorney learns of proposed corporate conduct or conduct by corporate employees that conflicts with her advice and that she believes is illegal, improper, or unwise, the professional rules provide several possible avenues through which the lawyer can attempt to persuade the client to change its plans. Under Model Rule 1.13:

If a lawyer for an organization knows that an officer, employee or other person associated with the organization is engaged in action, intends to act or refuses to act in a matter related to the representation that is a violation of a legal obligation to the organization, or a violation of law that reasonably might be imputed to the organization, and that is likely to result in substantial injury to the organization, then

28 See infra note 139–156 and accompanying text.
the lawyer shall proceed as is reasonably necessary in the best interests of the organization.\textsuperscript{30}

Let us suppose that a corporate lawyer deems it necessary that her client’s course of conduct change, but the officer with whom the lawyer is dealing demurs—for personal reasons or because the officer believes the corporation would benefit from rejecting the lawyer’s advice. In this instance, the lawyer can threaten a variety of steps short of revealing information to persons outside the corporation that might influence the officer to comply. Model Rule 1.13 authorizes the lawyer to inform a higher authority within the organization.\textsuperscript{31} Depending on the lawyer’s status within the organization, that may be an easy step for her to take, or it may risk her employment.\textsuperscript{32} Alternatively, the lawyer may inform a committee established within the organization charged with supervising law compliance.\textsuperscript{33} Or she may withdraw from representing the corporation in the matter\textsuperscript{34}—a dramatic step for in-house counsel because it is tantamount to resignation from her sole employment\textsuperscript{35} and may or may not exert significant influence on the client.\textsuperscript{36}

\textsuperscript{30} Id. at R. 1.13(b); cf. Model Rules of Prof’l Conduct R. 1.13(b) (1983) (requiring the lawyer to take some remedial steps, but leaving the remedy to the lawyer’s discretion).

\textsuperscript{31} Model Rules of Prof’l Conduct R. 1.13(b) (2002).

\textsuperscript{32} For example, a general counsel who is an officer of the corporation and questions the proposed actions of a lower-level employee may find it easy to raise the matter with the employee’s superiors. In contrast, a staff attorney faced with misconduct by a corporate vice-president may feel significantly intimidated by the prospect of challenging the vice-president’s conclusions to higher-ups.

\textsuperscript{33} Under the Sarbanes-Oxley regulations, for example, lawyers can sometimes obviate their own ethical responsibilities by informing an audit committee or a “qualified legal compliance committee” established for the purpose of evaluating disagreements about the propriety of the corporation’s conduct. See 17 C.F.R. §§ 205.3(b)(4), 205.3(c)(1) (2005) (stating that an attorney has fully satisfied her obligation if she reports a violation to a qualified legal compliance committee).

\textsuperscript{34} See Model Rules of Prof’l Conduct R. 1.16(b) (2002) (authorizing lawyers to withdraw when a client insists upon pursuing “repugnant” conduct); Model Rules of Prof’l Conduct R. 1.16(b)(3) (1983) (allowing attorney withdrawal based on “imprudent” client conduct).

\textsuperscript{35} See Stephen M. Bainbridge & Christina J. Johnson, Managerialism, Legal Ethics, and Sarbanes-Oxley Section 307, 2004 Mich. St. L. Rev. 299, 307 (arguing that the need of in-house counsel to please management will cause counsel to avoid pursuing management wrongdoing).

\textsuperscript{36} In other words, a corporation may not care if a particular lawyer resigns, especially when another equally qualified (but presumably more pliable) lawyer will take her place at no significant cost to the client. On the other hand, when a client has invested heavily in having one lawyer represent it, and substitution of counsel cannot be accomplished cheaply (or without substantial delay), then the client must balance the costs of losing the lawyer against the costs of following her advice.
Under some circumstances, counsel can up the ante. A mild step—one which enables in-house counsel to pass the buck somewhat or to enlist support for her opinion—is to suggest that the corporation seek an independent legal opinion.\textsuperscript{37} More forcefully, the lawyer can effectively require management to seek such an opinion, or to conduct an internal investigation, by issuing her own opinion stating that proposed conduct would breach management’s and the board of directors’ fiduciary duties.\textsuperscript{38} Proposed regulations under the Sarbanes-Oxley Act sometimes would also authorize the lawyer to exercise a “noisy withdrawal,” under which she resigns and disavows documents that represent or incorporate the improper conduct to an adversary, regulatory agency, or court.\textsuperscript{39} In the few circumstances in which a direct exception to confidentiality applies, the attorney may threaten to expose the client’s misconduct if the client does not accept her counsel.\textsuperscript{40}

Significantly, because of the context in which they offer representation, corporate counsel have a broader range of remedial options than lawyers confronting similar misconduct by individual clients. Law-

\textsuperscript{37} See Model Rules of Prof’l Conduct R. 1.13(b)(2) (1983) (listing the option of “advising that a separate legal opinion on the matter be sought for presentation to appropriate authority in the organization”).

\textsuperscript{38} When counsel issues such an opinion, even a CEO who intentionally plans to engage in questionable behavior would hesitate to proceed, because his defenses in a potential shareholder derivative or other suit may become limited and the board of directors similarly will be less likely to ratify his conduct. See A. Gilchrist Sparks, III & John F. Grossbauer, The Business Judgment Rule and Opinions of Counsel, \textit{in Corp. Law} 1987, at 756–58 (PLI Corporate Law Practice, Course Handbook Series No. B4-6813, 1987) (discussing the role of attorneys in advising corporate officers whether their conduct is likely to satisfy the business judgment rule). At a minimum, therefore, the CEO must take steps to obtain a second opinion that counteracts the effects of counsel’s initiative.

A similar process can occur in situations in which a corporation needs a favorable opinion of counsel in order to proceed with a legal filing or transaction. By withholding, or threatening to withhold, the opinion, counsel sometimes can force the client to amend its proposed course of conduct or, at a minimum, to seek a legal opinion from new counsel.


\textsuperscript{40} See Model Rules of Prof’l Conduct R. 1.13(c) (2002) (allowing a lawyer sometimes to reveal information when doing so will “prevent substantial injury to the organization”); \textit{see also} 17 C.F.R. § 205.3(d)(2) (2005) (providing that a lawyer may reveal confidential information to the Commission without the client’s consent to the extent the lawyer reasonably believes necessary “[t]o prevent the issuer from committing a material violation that is likely to cause substantial injury to the financial interest or property of the issuer or investors,” to prevent perjury, or to rectify the consequences of certain wrongdoing in furtherance of which the lawyer’s services were used).
yers for individuals essentially can only attempt to exert influence, withdraw, employ a noisy withdrawal when authorized to do so,\textsuperscript{41} or disclose if confidentiality exceptions permit. In most circumstances, noisy withdrawal is tantamount to disclosing the impropriety.\textsuperscript{42} Threatening either disclosure or noisy withdrawal is likely to carry significant weight and is likely to succeed in blackmailing compliance. The silent withdrawal alternative will be effective only when the client either places significant trust in this attorney or fears proceeding with new counsel.

II. CORPORATE LAWYERS’ INCENTIVES

In sorting out the reasons why lawyers would desire, or not desire, the power to force clients to accept legal advice, it is important to recognize that short- and long-term incentives differ. Threatening disclosure, for example, may enhance a lawyer’s immediate position or power in an organization, but in the long run may cause the organization to confide in, and depend on, the lawyer less frequently or to a lesser extent. Whether the individual lawyer would emphasize a short- or long-term view depends, at least in part, on the lawyer’s baseline expectations regarding her future relationship with the organization.\textsuperscript{43} As a result, what one might classify as a reason for some lawyers to desire a mandatory blackmail option sometimes also might be identified as a reason for other lawyers to wish that the option did not exist.

A. Economic Incentives

Corporate attorneys have some financial incentives to desire coercive power. First, it can be used to encourage corporate action that will entail the use of lawyers (for example, implementing a law compliance mechanism) or that may require the corporation to commission further legal work in the specific matter at issue.\textsuperscript{44} At least for

\textsuperscript{41} See Model Rules of Prof’l Conduct R. 1.6 cmt. (1983) (authorizing noisy withdrawals).

\textsuperscript{42} In other words, disavowing documents or aspects of representation alert the adversary that those items have caused a sufficient rift in the attorney-client relationship to justify the lawyer’s withdrawal.

\textsuperscript{43} See infra note 56–57 and accompanying text.

\textsuperscript{44} See Susan Saab Fortney, Chicken Little Lives: The Anticipated and Actual Effect of Sarbanes-Oxley on Corporate Lawyers’ Conduct, 33 Cap. U. L. Rev. 61, 75–76 (2004) (arguing that the increased focus on compliance enables the lawyer to bill more hours); Donald C. Langevoort & Robert K. Rasmussen, Skewing the Results: The Role of Lawyers in Transmitting Legal Rules, 5 S. Cal. Interdisc. L.J. 375, 377 (1997) (arguing that lawyers, particularly in
outside counsel, this would enhance the lawyer’s fee-earning capability. For inside counsel, exercise of the option highlights the lawyer’s importance in the organization and provides an opportunity for the lawyer to shine.

Second, both the existence of the option and its initial exercise increases the client’s immediate dependence on the lawyer. The client knows that future behavior must meet the lawyer’s approval. As a result, the lawyer’s position vis-à-vis the client generally, and in fee or salary negotiations specifically, is enhanced.

Third, in some jurisdictions, at least in-house counsel can use the tools made available through a blackmail option to immunize herself from discharge. In other words, to the extent a state allows corporate counsel to sue her employer for retaliatory discharge, the exercise of the lawyer’s threat is less easily punishable by the organization. Even if the organization has valid, separate reasons to discharge the attorney, the timing of a discharge following a lawyer’s threat will look suspicious. Manipulative corporate counsel thus can use the blackmail option to her economic advantage; in other words, to forestall discharge.

In the long term, the calculus is different. Under the traditional regime of loyalty and confidentiality, lawyers offer clients the valuable service of being intelligent sounding boards whose advice the client can accept or reject at will. That service is one of the reasons why corporate lawyers, in particular, are allowed to participate in a broad range of business decisions. To the extent lawyers gain the option, or are required, to control the client’s actions in these situations, the client will be less inclined to turn to the lawyer for advice until consultation is necessary for legal representation.

Moreover, the existence of coercive authority gives clients an incentive to minimize the information in a single lawyer’s hands. The

---


46 See Fisch & Rosen, supra note 8, at 1101, 1128 (arguing that mandatory blackmail provisions will reduce the information flow between attorneys and clients); Kaveh Noori-shad, The Sarbanes-Oxley Act and In-House Legal Counsel: Suggestions for Viable Compliance, 18 GEO. J. LEGAL ETHICS 1041, 1050 (2005) (arguing that Sarbanes-Oxley may cause issuers to give attorneys less information); cf. Kostant, supra note 8, at 550–51 (arguing that there is no empirical evidence to support the notion that lawyers will be kept out of the loop by the
more a lawyer knows about the client’s overall practices, the more likely it is that a blackmail option will be triggered. Clients therefore become well-advised to spread legal work around, rather than to assign it to a single lawyer. This works to the disadvantage of in-house counsel and law firms that represent individual corporations on an ongoing basis, but may help firms that tend to perform spot work.

Clients also may make distinctions in when they consult counsel. Many, perhaps even most, clients will continue to ask lawyers before the fact about the potential illegality of future or hypothetical behavior. The clients have an acute interest in knowing the consequences of proposed action. If they confine the inquiry to this stage, the lawyer will have no basis for questioning the corporation’s conduct or making a report up the ladder. Only when a client subsequently informs the lawyer about what it has done, or includes the lawyer in subsequent decision making, does the blackmail option present any risk. Accordingly, one would expect many clients to alter their use of lawyers to conform to this model.

These phenomena may be especially significant to in-house counsel who play a dual role in corporations—part legal advisor and part participant in the business activities of the corporations. Small corporations sometimes cannot economically justify full-time legal staffs and thus expect line attorneys to perform business functions as well. In larger corporations, staff counsel—or even the general counsel—may perceive their position as a stepping-stone for obtaining business expertise and eventually moving up in the corporate hierarchy in a non-legal capacity. A corporation that fears providing business-related information to lawyers (i.e., because the professional rules may in the future require the lawyers to react to the information) will hesitate to employ lawyers in a dual capacity. The coercive rules thus may enhance the status of lawyers as lawyers in the corporation, but reduce their economic opportunities as current or future businesspersons.

Finally, it is important to note that changes in the working relationship between client and lawyers also may affect the closeness of the

---

47 See John C. Coffee, Jr., Gatekeeper Failure and Reform: The Challenge of Fashioning Relevant Reforms, 84 B.U. L. Rev. 301, 362 (2004) (arguing that under coercive rules, clients will ask lawyers to advise them regarding future hypothetical conduct, but refrain from discussing actual conduct post hoc for fear that the attorney will need to disclose).

48 Cf. Deborah A. DeMott, The Discrete Roles of General Counsel, 74 Fordham L. Rev. 955, 958–61 (2005) (discussing the way the roles played by in-house counsel have changed during different periods of American history).
relationship. Clients who become less dependent on individual lawyers and have less of a history of dealing with them on a regular, intimate basis are less likely to view the lawyers they do retain as essential allies in their working routine. Consequently, the work assigned, and fees paid, to individual lawyers by single companies are likely to decrease.

B. Incentives Relating to Status Within the Organization

The existence of coercive power is likely to affect the status of corporate attorneys, sometimes positively, sometimes negatively. On a simple level, authorizing lawyers to supervise an organization’s conduct increases the importance of the lawyer as a decision maker within the organization.49 Once the organization decides to include the lawyer in addressing a matter, the organization must be prepared to heed the lawyer’s advice.50 That is not necessarily the case with respect to other, low-level employees.51

Moreover, in some jurisdictions, the requirement that a lawyer respond to specific types of corporate conduct extends to business decisions, not merely decisions concerning the application of law. Under California’s organizational attorney rule, for example, the lawyer may take remedial action whenever an agent of the organization “intends . . . to act . . . in a manner which is likely to result in substantial injury to the organization.”52 This language suggests to agents of the company that a lawyer who disagrees with the agent’s assessment of the effect of a particular business decision is authorized to, and should, go over the agent’s head.

The existence of coercive authority thus enhances the lawyer’s immediate position in the organization in two ways. First, it makes the lawyer’s advice more important than it might be if offered by laypersons within the organization. Second, it suggests that the lawyer has a place in the corporate decision-making process at least equal to that

49 As will be discussed, however, the issue is more complex than it appears at first glance because the existence of the authority may cause the organization to use a lawyer less. See infra note 56–57 and accompanying text.

50 Fortney, supra note 44, at 75 (noting that the Sarbanes-Oxley regulations give attorneys “leverage” in dealing with management).

51 Corporations, of course, accept or reject the advice of ordinary employees at will. Such employees ordinarily are bound by a duty of loyalty (i.e., under agency law) not to reveal the information outside the organization, at pain of dismissal. Unless they personally participate in corporate misconduct, these employees ordinarily have no legal obligation to pursue issues beyond the level of their own superiors.

52 Cal. Rules of Prof’l Conduct R. 3-600(B) (2004).
of the corporate agent seeking advice.\textsuperscript{53} Especially once the lawyer exercises coercion, these effects may enhance the lawyer’s image both inside\textsuperscript{54} and outside\textsuperscript{55} the organization.

The picture begins to change as this culture of legal representation matures. The more that lawyers are perceived to be potential monitors of the organization rather than team players within it, the more likely they are to become marginalized.\textsuperscript{56} They will still be used to perform legal work because clients have no choice but to obtain representation when necessary to resolve active cases. To expand their duties within an organization, however, lawyers will have to prove their value based on characteristics other than their trustworthiness and loyalty.

These considerations probably are more significant for in-house counsel. For reasons already discussed,\textsuperscript{57} organizations faced with a serious possibility of being coerced have incentives to spread legal work among various lawyers and to cabin the information each lawyer receives. This militates in favor of sending work to varied external counsel.

The marginalization likely will affect line attorneys more than a general counsel who already is high enough in the organization to be assured a voice in decision making. A general counsel often has become a member of the management team and is perceived to have personal incentives that ally him with management—including having

\textsuperscript{53} I do not mean to suggest that the lawyer necessarily will have the same power as the corporate officer. Whether persons higher up in the management hierarchy will listen to the lawyer or the officer depends, in large measure, on whom they trust more. What does change in the relationship, however, is that the lawyer gains access, or lines of communication, to persons higher in the chain of command than the lawyer might have had without the authority granted in the rules.

\textsuperscript{54} Once a lawyer’s decision to act upon blackmail authority becomes known within the organization, the lawyer’s visibility is enhanced. For example, had a lawyer for Enron protested its accounting practices and taken steps to challenge their validity within the firm without repercussion, the lawyer quickly would have been perceived within the organization as a person of status.

\textsuperscript{55} To the extent that the outside world’s expectation is that the lawyer’s word must be heeded, the lawyer will be treated as a more important, and better qualified, player. This is especially the case in jurisdictions in which the rules specifically assign corporate lawyers a blackmail-supported role in evaluating the corporation’s business, as well as legal, decisions.

\textsuperscript{56} Cf. Geoffrey C. Hazard, Jr., Ethical Dilemmas of Corporate Counsel, 46 Emory L.J. 1011, 1017 (1997) ("Lawyers in a corporate law department, as they are often reminded, are part of the ‘corporate team.’").

\textsuperscript{57} See supra note 46 and accompanying text.
more to lose from opposing management’s position. In contrast, there may be less reason for management to trust line attorneys and empower them to act against management’s interests.

The effects of providing coercive authority also may vary depending on whether in-house counsel is a supervisory or subordinate attorney, especially in large companies. A staff attorney, in essence, serves two masters—her boss and the company (i.e., the boss’s boss). Some blackmail rules permit such lower-level employees to satisfy their responsibilities either by reporting to their immediate superiors or by pursuing the matter further, which may displease the supervising attorney but may be in the company’s best interests. Other rules require line attorneys to pursue the matter all the way up the ladder. The issue of how a blackmail option affects the line attorney’s status within the organization thus becomes exceptionally complicated and turns, in part, on the precise phrasing of each blackmail rule.

In general, enhancing lawyers’ coercive authority will adversely affect in-house attorneys’ personal relationships within the corporation. Even low-ranking employees are more likely to shy from confiding in in-house counsel than before. Consider, for example, an employee in an Enron-like scenario who has doubts about his employer’s accounting practices. Would that employee be more likely to discuss the matter with a non-lawyer co-worker who shares his interests (for example, in doing his best for the company but also maintaining his position in the company) or with a lawyer freighted with the obligation to act on information regarding wrongdoing? The answer, of course, depends partly on whether the lawyer’s coercive authority is mandatory or discretionary in nature. Yet it seems clear that

58 See George M. Cohen, When Law and Economics Met Professional Responsibility, 67 Fordham L. Rev. 273, 284 (1998) (noting that corporate clients face “agency costs from not only the managers, whose self-interest gave rise to agency theory in the first place, but also from in-house counsel”).

59 See 17 C.F.R. § 205.5 (2005) (stating that subordinate attorneys need only report evidence of a material violation to their supervising attorney, but if they reasonably believe the supervising attorney has failed to comply with the rule the subordinate has the option of reporting up the corporate ladder); cf. Model Rules of Prof’l Conduct R. 5.2 (2002) (providing that a subordinate lawyer does not violate the professional rules when she “acts in accordance with a supervisory lawyer’s reasonable resolution of an arguable question of professional duty”).

60 See Model Rules of Prof’l Conduct R. 1.13(b)–(c) (2002) (requiring lawyers to pursue the matter to “highest” authority).

61 This analysis, of course, assumes that the corporation and its employees perceive the possibility that the company’s lawyers sometimes will exercise their coercive authority.
the employee’s general sense of how lawyers act, or must act, will affect the employee’s attitude towards staff counsel.\textsuperscript{62}

C. Personal Incentives

Corporate lawyers may desire coercive authority for purely psychological reasons. The existence of the power may enhance their sense of self-worth. It may reassure them that their role as an attorney does not undermine their own ability to act as moral individuals.

They also have several personal incentives to exercise the power. In the individual case, forcing the organization to act in a moral or legal way may, for the lawyer, be equivalent to acting morally herself. It may also make it easier for the lawyer to avoid personal legal liability for knowing of, or participating in, corporate misconduct. To the extent the lawyer’s actions become public, the lawyer’s behavior may enhance her personal reputation.

It therefore seems surprising that many lawyers are entrenched in their opposition to rules that would establish coercive authority, especially new exceptions to attorney-client confidentiality.\textsuperscript{63} One reason may be that with authority potentially comes responsibility. Strict rules requiring lawyers to act in accordance with their clients’ desires serve as a protective shield for lawyers.\textsuperscript{64} In contrast, the existence of a blackmail option may open lawyers to personal liability to third per-

\textsuperscript{62}See Hazard, \textit{supra} note 56, at 1018–19 (analyzing and distinguishing the practice of in-house and external counsel in terms of their “water cooler” and “back-channel” interactions with other corporate employees and the information available to counsel through such interactions).

\textsuperscript{63}California attorneys who until the year 2004 were governed by a nearly absolute confidentiality rule, for example, consistently fought against a future crime exception and the disclosure requirements of Sarbanes-Oxley. \textit{Cf.} Letter from the State Bar of Cal., Bus. Law Section, Corp. Comm., to Giovanni P. Prezioso, General Counsel, U.S. Sec. & Exch. Comm’n (Aug. 13, 2003), \textit{available at} http://www.calbar.ca.gov/calbar/pdfs/sections/buslaw/corporations/2003-10-08_SEC.pdf (arguing that stricter California confidentiality rules should trump the Sarbanes-Oxley requirements).

\textsuperscript{64}One of the major concerns on the floor of the American Law Institute (the “ALI”) debate concerning, inter alia, confidentiality exceptions was the potential for liability that discretionary exceptions make possible. \textit{See Restatement (Third) of the Law Governing Lawyers} §§ 66(3), 67(4) (2000) (providing that a lawyer who “takes action or decides not to take action permitted under [a crime or fraud exception to confidentiality] is not, solely by reason of such action or inaction, . . . liable for damages”); \textit{cf. id.} § 54(1) (providing that “[a] lawyer is not liable under § 48 or § 49 for any action or inaction the lawyer reasonably believed to be required by law, including a professional rule”). Some members of the ALI argued that lawyers should be immunized from liability more generally whenever they exercise discretion that the professional rules accord.
sons should they fail to take appropriate action. Lawyers governed by limiting but lawyer-protective rules thus have strong incentives to disfavor the extension of coercive power.

The ability to “blackmail” clients into acting in an appropriate fashion, especially if discretionary, also will impose psychological burdens on some lawyers. It requires lawyers to make potentially difficult moral decisions, including decisions that can be unpleasant for the client. Even a lawyer who adopts a rule of thumb that she will always act in the way that the client wishes must at least make that decision consciously. Arguably, discretionary rules may require more case-by-case introspection. A non-discretionary rule in either direction (that is, one requiring or forbidding lawyer action) essentially allows lawyers to remain amoral and to attribute any bad results to their role in the legal system.

Lastly, according coercive authority weakens lawyers’ ability to perceive themselves as the client’s friend and ally. Particularly in-house counsel, who has a single client and spends each day in the client’s workplace, may come to feel like an outsider. She no longer can be one of the team, because she has a special obligation to monitor the other employees.

D. Outward-Looking Incentives

Some lawyers may desire coercive power for reasons independent of their personal interests. Most of the rules that explicitly authorize lawyers to force clients to take particular actions—like the Sarbanes-Oxley regulations—stem from an assessment that the actions required of lawyers will promote socially beneficial conduct that is more important than the harm the actions might inflict on clients or the attorney-

65 Discretionary authority to reveal a client’s intent to harm a third person can help support an injured third party’s contention that liability under Tarasoff v. Regents of the University of California should ensue upon the lawyer’s failure to prevent the harm. See Fred C. Zacharias, Privilege and Confidentiality in California, 28 U.C. Davis L. Rev. 367, 405 (1995) (discussing the relationship between confidentiality exceptions and Tarasoff liability). See generally Tarasoff v. Regents of the Univ. of Cal., 551 P.2d 334 (Cal. 1976).

66 As discussed below, there is room for disagreement about whether discretionary rules require lawyers to exercise the discretion in each case or whether the grant of discretion leaves the lawyer free to adopt any approach. See infra notes 159–160 and accompanying text.

67 See, e.g., Charles W. Wolfram, Modern Legal Ethics, § 6.1, at 247 (1986) (discussing confidentiality as a shield for lawyers); Zacharias, supra note 4, at 373 nn.97–101 (listing authorities that discuss the personal consequences of strict confidentiality rules).
client relationship. Some lawyers share this assessment. In other words, they too believe that preventing immoral or illegal client conduct (or promoting moral or legal conduct) justifies occasional coercion. Such lawyers, at least, will have the desire for, and the incentive to exercise, a blackmail option in order to serve societal interests.

III. SOME RAMIFICATIONS OF THE COMPETING INCENTIVES

Different forms of coercive authority will affect lawyer behavior in different ways. On the surface, authorizing lawyers to force client conduct seems only to heighten the status of lawyers in the attorney-client relationship and to enable them to exercise individual moral decision making. This seems most apt when the authority is discretionary. The presence of discretionary authority, however, may influence how lawyers act within the attorney-client relationship. The responsibilities that come with the authority may cause lawyers to oppose or avoid implementing an option to blackmail.

First and foremost, a lawyer who has the option to force clients to act in a certain way has psychological burdens that do not affect lawyers bound to secrecy or strict notions of “loyalty.” The lawyer must deal directly with moral issues. She potentially also must consider whether to exercise coercion upon clients with whom she has built a personal relationship, perhaps even friendship.

More importantly, the existence of discretionary authority exposes the lawyer to the possibility of liability for failing to take action. One of the keys to the California Supreme Court’s 1976 decision in

68 See Richard W. Painter, Standing up to Wall Street (and Congress), 101 Mich. L. Rev. 1512, 1520–21 (2003) (book review) (citing Letter from Richard W. Painter et al., to Harvey Pitt, Chairman, Sec. & Exch. Comm’n (Mar. 7, 2002), signed by forty law professors “seeking a [SEC] rule requiring issuers’ lawyers to report unrectified securities law violations to client boards of directors”); Ahuja, supra note 8, at 1333 (arguing that a requirement to report up the ladder serves the public interest and increases confidence in the legal profession); Developments in the Law—Corporations and Society, 117 Harv. L. Rev. 2227, 2234–37, 2248 (2004) (arguing that a lawyer’s responsibility to the public sometimes must transcend the attorney-client relationship and that neither the current Model Rule 1.13 nor Sarbanes-Oxley go far enough); cf. Richard W. Painter, Convergence and Competition in Rules Governing Lawyers and Auditors, 29 J. Corp. L. 397, 410 (2004) (suggesting that, although it is too early to reach a verdict on Sarbanes-Oxley, customized solutions for each lawyer-client relationship may be more effective than an all encompassing solution).

69 Of course, a lawyer or law firm may adopt the position that it will always exercise discretion in accordance with the client’s will. Even if such attorneys can avoid making moral decisions on a case-by-case basis, however, the attorney must at least make the initial determination to cede moral independence. But see infra note 159 and accompanying text (questioning whether lawyers may cede discretionary authority).
Tarasoff v. Regents of the University of California, the case providing the legal basis for psychiatrist liability for failure to disclose danger created by patients, was the existence of professional rules that allowed disclosure.\textsuperscript{70}

Thus, despite the initial attractiveness of the enhancement of their status through the grant of discretionary authority, lawyers may seek to avoid situations that trigger coercive authority. They can do so in two ways. First, lawyers can warn a client not to advise them of triggering information.\textsuperscript{71} Second, they can avoid participating in tasks that are likely to put them in an awkward position.\textsuperscript{72}

The nature of the triggering mechanism is key to lawyers’ ability to skirt coercive rules. Most such rules depend on lawyers’ “knowing” of client wrongdoing\textsuperscript{73} or being aware of “credible evidence” of wrongdoing that would be “unreasonable” for them to ignore.\textsuperscript{74} In the Enron setting, for example, lawyers for the corporation and auditing accountants were able to convince themselves—and argue after the fact—that, although they might have suspected some of the client’s practices, they had a right to rely on the client’s factual representations and thus did not “know” of any wrongdoing.\textsuperscript{75} Likewise, even under the subsequent Sarbanes-Oxley regulation, lawyers in Enron-like situations still can take the position that accepting the client’s word ordinarily is not “unreasonable.”\textsuperscript{76}

\textsuperscript{70} See 551 P.2d 334, 347 (Cal. 1976).

\textsuperscript{71} See Robert W. Gordon, A New Role for Lawyers? The Corporate Counselor After Enron, 35 Conn. L. Rev. 1185, 1202–03 (2003) (arguing that lawyers involved with Enron consciously avoided learning the facts in order to avoid complicity).

\textsuperscript{72} Cf. Cohen, supra note 58, at 282 (noting that lawyers may “act in a self-interested way to use their informational advantage [for example, information gained through attorney-client confidentiality] to evade their responsibilities to their clients . . . [and] to help their clients evade their responsibilities towards others”); James D. Cox, Managing and Monitoring Conflicts of Interest: Empowering the Outside Directors with Independent Counsel, 48 Vill. L. Rev. 1077, 1092 (2003) (advising corporate lawyers to refrain from scrutinizing closely an issuer’s transactions to avoid triggering Sarbanes-Oxley’s requirements).

\textsuperscript{73} See, e.g., Model Rules of Prof’l Conduct R. 1.6(b) (2002) (allowing disclosure when the lawyer “reasonably believes” it is “necessary” to prevent particular “reasonably certain” results); id. at R. 1.13(b) (requiring lawyer to act when she “knows” corporate officers are acting or intend to act in the prohibited fashion); id. at R. 3.3(b) (requiring lawyer to act when she “knows” that “a person intends to engage, is engaging, or has engaged in criminal or fraudulent conduct related to the proceeding”).

\textsuperscript{74} See 17 C.F.R. § 205.2(e) (2005).


\textsuperscript{76} See Susan P. Koniak, When the Hurlyburly’s Done: The Bar’s Struggle with the SEC., 103 Colum. L. Rev. 1236, 1275–76 (2003) (discussing weaknesses of the trigger requirements of the Sarbanes-Oxley regulations); see also Cramton et al., supra note 11, at 752 (arguing
When the disclosure authority is mandatory, some of the same considerations apply. The psychological burdens may be less, because the lawyer has no choice but to exercise the authority when the trigger is satisfied. The malleability of most triggers, however, continues to allow wiggle room. Moreover, the lawyer still must be cognizant of her potential legal liability. She therefore also may take steps to avoid blackmail situations.

Under a mandatory regime, the lawyer must consider whether her obligations to the client include warning the client of the blackmail option in advance—that is, “mirandizing” the client—and avoiding participation in potential blackmail situations. Some commentators have suggested, for example, that a lawyer must advise the client of the existence of confidentiality exceptions, even if she does not need to spell out how the client can avoid their application.\textsuperscript{77}

In-house counsel, especially one who is herself an officer or supervisory attorney, must internalize the potential operation of a mandatory rule on her working relationship with others in the organization. A mandatory rule, in essence, may require her routinely to go over the heads of other employees with whom she deals on a day-to-day basis. To the extent a good working relationship with the other employees is important for the lawyer’s job performance, she has a

\textsuperscript{77} \textit{See}, e.g., H. Lowell Brown, \textit{The Crime-Fraud Exception to the Attorney-Client Privilege in the Context of Corporate Counseling}, 87 Ky. L.J. 1191, 1198 n.19 (1999) (noting that “it has been observed that attorneys should give ‘Miranda-like warnings’ when counseling clients’); Max D. Stern & David A. Hoffman, \textit{Privileged Informers: The Attorney Subpoena Problem and a Proposal for Reform}, 136 U. Pa. L. Rev. 1783, 1804 (1988) (arguing that attorneys should warn clients about the manner in which client disclosures may not be privileged); Zacharias, \textit{supra} note 4, at 387 (discussing the relationship between client autonomy and advising clients about confidentiality exceptions); cf. David Binder & Susan Price, \textit{Legal Interviewing and Counseling: A Client Centered Approach} 108 (1977) (proposing a specific promise to be given to clients that “I cannot and will not divulge anything you say to anyone else without your express permission’’); Freyman & Smith, \textit{supra} note 16, at 161–62 (arguing against saying anything to clients about exceptions to confidentiality because that would chill the attorney-client relationship). \textit{See generally} Lee A. Pizzimenti, \textit{The Lawyer’s Duty to Warn Clients About Limits on Confidentiality}, 39 Cath. U. L. Rev. 441 (1990) (discussing the duty to warn clients). California’s recently amended confidentiality exception for future crimes, however, seems to envision lawyers sometimes intentionally withholding information about the exception until the client has already revealed the confidence to the lawyer. \textit{Cal. Rules of Prof’l Conduct} R. 3-100 discussion ¶ 9 (2004) (authorizing lawyers not to advise clients because “under certain circumstances, informing a client of the member’s ability or decision to reveal confidential information . . . would likely increase the risk of death or substantial bodily harm”).
special reason to avoid situations in which coercive authority is triggered. The lawyer thus has incentives not only to avoid information, but also to train employee-clients to ask questions and seek advice in a form that will not satisfy the trigger.78

On the surface, the combination of the triggering mechanisms and the ability of lawyers and clients to signal their desires looks like a simple phenomenon to analyze. Lawyers and clients will decide what they want from one another and let the other know in time for the other to shape his or her behavior. Consider this added complication, however. Transactions often are ongoing. Triggers for different lawyer obligations and authority may occur at various times during a transaction, as may the opportunity for signaling.

Thus, for example, the new version of Model Rule 1.6 authorizes lawyers to make disclosures they “reasonably believe necessary” to prevent crimes or frauds in which the lawyer’s services have been “used.”79 A client might obtain initial advice from a lawyer but then, by excluding her from the actual decision to propose or initiate the conduct or by screening her from details about its execution, avoid putting the lawyer in a position to disclose. After a transaction is complete, clients sometimes may also have incentives to keep their lawyer in the dark about what has occurred, because the self-defense exception in Model Rule 1.6(b)(5) (especially combined with the new authority to prevent harms in Model Rule 1.6(b)(3)) can subsequently empower the lawyer to act coercively.80 Controlling the lawyer might be more difficult, however, under Model Rule 1.13, which authorizes the lawyer to act when she “knows” that an officer engages or “intends” to engage in specified misconduct.81 Although the knowledge threshold is higher than under Model Rule 1.6, once the lawyer

---

78 Thus, for example, lawyers may advise clients to seek advice through hypothetical questions or other mechanisms that enable the lawyers to avoid knowing, or having credible evidence, that the client has, or proposes to, engage in wrongdoing. Cf. Koniak, supra note 76, at 1271 (arguing that “lawyers never ‘know’ that their client is committing a crime or fraud, not before a court has ruled that way”).

79 Model Rules of Prof’l Conduct R. 1.6(b)(2)–(3) (2002).

80 See id. at R. 1.6(b)(5) (allowing lawyers to disclose to “respond to allegations in any proceeding concerning the lawyer’s representation of the client”); id. at R. 1.6(b)(3) (authorizing disclosures to “prevent, mitigate or rectify substantial injury to the financial interests . . . of another that is reasonably certain to result or that has resulted from” a crime or fraud in which “the client has used the lawyer’s services”); cf. Meyerhofer v. Empire Fire & Marine Ins. Co., 497 F.2d 1190, 1194–95 (2d Cir. 1974) (finding no violation of professional rules in former lawyer’s disclosure of fraud when lawyer faced threat of being named as a defendant in a securities class action).

knows of a corporate agent’s *intent* to act wrongfully, the agent’s decision to dismiss or screen the lawyer may not be sufficient to obviate the lawyer’s power, because the lawyer continues to have obligations to the actual client, the corporation. Thus, at each stage of their transactions, sophisticated lawyers and clients are likely to be aware of the different triggers and accordingly will cooperatively limit the knowledge transmitted to lawyers. The willingness of lawyers to signal to clients how they should act may become an important part of the attorney-client relationship.

Finally, the mere potential for the exercise of coercive power over the corporation—whether discretionary or mandatory—may function as an economic glass ceiling for in-house lawyers, particularly low-level staff attorneys. It provides incentives for organizations to farm out work. Perhaps more significantly, it gives corporations a disincentive to training and including line attorneys in non-legal roles.

These considerations help explain why lawyers might oppose regulation embodying coercive authority even when the regulation seems to enhance the lawyers’ personal power. There are idealistic justifications for opposing blackmail rules; namely, that the rules negatively affect the traditional attorney-client trust relationship that allegedly lies at the heart of adversary ethics. More personally, however, blackmail rules can negatively affect lawyers’ interpersonal connections with clients and their status within a client organization. They affect both how a lawyer will be approached by an organization’s employees and the work she will (and should) receive.

Let us consider a bit more specifically the four most commonly discussed forms of corporate blackmail rules, each with two variations, and consider their likely impact on lawyers and clients. These include rules giving corporate counsel discretion to threaten remedial action, rules requiring lawyers to go up the ladder, rules requiring disclosure, and rules requiring noisy withdrawal.

---

82 An example of a client’s attempt to follow such a procedure is found in Balla v. Gambro, Inc., 584 N.E.2d 104, 106 (Ill. 1991), in which the client promised the lawyer not to ship defective dialysis machines, but then did so nonetheless.

83 See *supra* note 47–48 and accompanying text (discussing the business role of many in-house lawyers).

84 See Freedman & Smith, *supra* note 16, at 49–51 (discussing the importance of client autonomy in the attorney-client relationship).
A. Discretionary Rules

Under the old version of Model Rule 1.13, still in effect in many states, lawyers who learn of corporate illegality must take action, but are given broad discretion regarding what steps to take. The ability of a lawyer to coerce client conduct by threatening to take action is limited in two ways. First, the lawyer may only proceed "in the best interest of the organization," not that of society as a whole. Second, the lawyer’s actions may not involve the disclosure of confidences.

This version of coercive authority maximizes the ability of officers and employees to trust and use the corporate lawyer. Ordinarily, officers and employees will be acting (or think they are acting) in the best interests of the company, and so can be confident that they can prevent the lawyer from embarrassing them (for example, by going over their heads). Indeed, the threat of lawyer action probably is less than the parallel threat from other non-lawyer employees who have the same information, because the lawyer’s ability to sue for retaliatory discharge when sanctioned for acting is more limited. Lawyers actually have more to fear than other employees if they exercise a blackmail option. Model Rule 1.13’s express limitation on lawyer disclosures further constrains the threat that lawyers pose.

As a consequence, it is fair to conclude that the old version of the rule will maximize corporate clients’ use of lawyers and will maximize the economic interests of corporate attorneys. On the other hand, it limits attorneys’ independence and status, at least in the case of in-house counsel. External counsel have one potentially effective coercive option available: namely, the ability to resign, if they are willing to lose a single client. In some jurisdictions, this ability to resign is accompanied by the right to disavow fraudulent documents that the lawyers have helped prepare or with respect to which the lawyer’s ser-

---


86 MODEL RULES OF PROF’L CONDUCT R. 1.13(b) (1983) (listing options that required remediation "may include").

87 Id.

88 Id. at R. 1.13 cmt. (noting that “this Rule does not limit or expand the lawyer’s responsibility under 1.6”).

89 See Sara A. Corello, Note, In-House Counsel’s Right to Sue for Retaliatory Discharge, 92 COLUM. L. REV. 389, 405 (1992) (noting that attorneys may be more vulnerable to corporate pressure than non-lawyer personnel who have standing to sue for retaliatory discharge after blowing the whistle).
vices otherwise have been used. Although in-house counsel have the same option, they are far less likely to exercise it because of their dependence on the single employer.

By making the choice of remedy other than disclosure discretionary, the old Model Rule 1.13 allows corporate officers to pressure a lawyer into selecting the option that least disrupts their plans. Because the rules do not require, or even give the lawyer the wherewithal, to prevent misconduct unilaterally (for example, through disclosure), the lawyer’s natural incentives are to balance her obligation to counteract misconduct against her own interests. Those interests ordinarily will be to ally herself with management and to pursue the desires of those officers who control her employment.

The same syllogism applies to line attorneys who can satisfy their obligations by reporting an issue to supervisory attorneys (or by consulting outside counsel). Although they may be authorized to go over their superiors’ heads, there will be ramifications for doing so. The line attorney’s personal interests are maximized by allowing the superior to control the moral decision.

The relationship between management and attorney becomes far more complicated under variations of the rule—like new Model Rule 1.13—that allow (but do not require) disclosure when the company does not adhere to the lawyer’s wishes. This approach at once requires supervisory or outside lawyers actually to confront moral dilemmas when a client insists on pursuing fraudulent or illegal conduct and puts these lawyers at risk of personal sanction if they fail to act. The lawyers can internalize this risk in one of two ways. They may exercise coercion, which in the long run may cost them the client or status in the firm. Alternatively, they can exact payment for assum-

---

90 See Model Rules of Prof’l Conduct R. 1.6 cmt. (1983) (providing that a lawyer may “withdraw or disaffirm any opinion, document, affirmation, or the like”).
91 See Developments in the Law—Corporations and Society, supra note 68, at 2246 (arguing that absent a mandatory rule, lawyers will focus on pleasing management).
93 See Douglas Michael McManamon, Comment, Should Attorneys Be Footsoldiers in the War on Corporate Fraud?, 38 U.S.F. L. Rev. 163, 183 (2003) (arguing that, under the Sarbanes-Oxley regulations, junior attorneys most likely will limit themselves to advising a supervising attorney of corporate misconduct).
94 See supra notes 69–70 and accompanying text.
ing the risk by signaling to the managers that they will not exercise the option in exchange for reciprocal loyalty on the managers’ part.\textsuperscript{95}

One might, therefore, expect the bar to splinter in its view of the desirability of this option. Lawyers who are not prepared to agree to act complicitly with clients and who take their moral obligations seriously actually should prefer not to have the discretionary disclosure option, because it would hurt them economically. In contrast, the option gives a competitive advantage to lawyers willing to cede their discretion.

Clients, too, are likely to respond in varying ways. If the corporate officer in charge of retaining counsel is committed to ensuring the legality of corporate conduct, he will prefer the lawyer who potentially might disclose. On the other hand, the officer who emphasizes personal loyalty is likely to gravitate to the lawyer willing to bargain away her moral authority.

\textbf{B. Rules Requiring Lawyers to “Report up the Ladder”}

A second form of corporate blackmail, reflected in the new Model Rule 1.13 and the Sarbanes-Oxley regulations, establishes a presumption that corporate lawyers must report “up the ladder” when they learn of inappropriate corporate conduct and must pursue the climb to higher authorities until they are satisfied.\textsuperscript{96} The Sarbanes-Oxley regulations differ from Model Rule 1.13 in one important respect: a lawyer may shortcut her obligation to climb the ladder if the corporation has established a qualified legal compliance committee (the “QLCC”) and the lawyer reports to it. California adopts a different variation of Model Rule 1.13. It requires the lawyer to report, at most, to the corporation’s highest “internal authority,”\textsuperscript{97} presumably excepting independent or public boards of directors that might not be in a position to keep sensitive information confidential.\textsuperscript{98}

\begin{flushleft}
\textsuperscript{95} Cf. McGowan, supra note 12, at 1825–26 (assuming that, at least for disciplinary purposes, lawyers have total discretion in deciding when to implement discretionary disclosure options and that lawyers will make economically rational decisions about implementation).
\textsuperscript{96} 17 C.F.R. §§ 205.2(b), 205.3(b)(1) (2005); Model Rules of Prof’l Conduct R. 1.13(b) (2002).
\textsuperscript{97} Cal. Rules of Prof’l Conduct R. 3-600(B)(2).
\textsuperscript{98} See id. There are no cases or legislative history interpreting the “highest internal authority” language of R. 3-600(B)(2). The language, however, was adopted in 1989 to contrast with the then-existing Model Rule 1.13, which did not confine disclosure to internal management. California’s heavy emphasis on securing attorney-client confidentiality elsewhere in its professional rules supports the notion that Rule 3-600’s language was intended
\end{flushleft}
These rules all share a common trait. They are not discretionary, except in the sense that they allow the lawyer to make the initial determination that the reporting requirements are triggered. Once the trigger is satisfied, the lawyer must report and must (except under the Sarbanes-Oxley compliance committee safe harbor) continue to press her view to the highest corporate authorities unless her view is satisfied or she becomes convinced that she was in error.

The absence of discretion has several effects. It minimizes the psychological burdens that choices impose on lawyers. It makes clear to corporate employers the benefits of not conveying information to lawyers, or of cabining the information multiple lawyers receive. It may make the use of one-time outside counsel attractive, because outside counsel can both be dealt with on a need-to-know basis and discharged more easily than full-time counsel. It also encourages organizations to use non-lawyers to fulfill tasks when possible.

When one adds the substitute option of reporting to a QLCC or other internal compliance committee, however, the calculation changes dramatically. Three sets of questions become important. First, is the lawyer personally better off flexing her own muscles (that is, by insisting upon her position up the ladder) or handing off the problem to a committee that will assume the legal and moral responsibility inherent in the blackmail paradigm? Second, is the organization better off having a lawyer or the committee address the matter? Third, and perhaps most important, to what extent can the organization signal its preference to the lawyer and will the lawyer honor that signal?

The existence of the committee structure may be especially attractive to in-house counsel, because it provides an alternative to the use of multiple outside counsel. If corporate management is satisfied that a QLCC, for example, will look after its interests, then inside counsel can inform the management in advance of her preference for its use and thereby fend off the competition of outside counsel and maintain her status within the corporation.\textsuperscript{99} In another sense, the existence of the QLCC as an option provides corporate counsel with the ability to make personal tactical choices about when referring an

\textsuperscript{99} Cf. Jill Fisch & Caroline M. Gentile, \textit{The Qualified Legal Compliance Committee: Using the Attorney Conduct Rules to Restructure the Board of Directors}, 53 \textit{Duke L.J.} 517, 536, 546 (2003) (noting that attorneys have an incentive to encourage clients to establish QLCCs because they minimize the attorney’s obligations).
issue to the QLCC will insulate her from criticism and when it will enhance her power.  

More likely, however, is the possibility that the corporation itself will develop a culture. An organization that wishes to avoid independent analysis of the legality of its operations will establish a QLCC that is deferential, and will signal to its lawyers that any questions should be delivered to the committee. It is easy to provide and enforce such signals to inside counsel. The opportunities for rewarding salaried employees (for example, through promotions and bonuses) are frequent.

A course of conduct may be more difficult to establish with outside lawyers unfamiliar with the corporation’s routine. Arguably, sophisticated outside counsel can easily and quickly discern management’s desires regarding independent investigating committees. Management’s willingness to risk a signal, however, may depend either upon the existence of a previous relationship with external counsel or upon the external counsel’s reputation for willingness to accept a signal and abide by client desires.

One might assume that management always will hire a law firm with a reputation for malleability and that all economically rational law firms will signal their malleability. But the accuracy of that proposition may well vary with the context in which a firm is hired. When, for example, a corporate client expects a court or administrative agency to shine a spotlight on its actions (e.g., because a shareholder suit has been or will be filed or because an agency has announced plans to scrutinize this category of transaction), the corporation might prefer to engage counsel with a reputation for independence and objectivity. Conversely, a law firm’s overall marketability may

100 See id.

101 See Henning, supra note 21, at 376 (“Lawyers are not immune to being co-opted into a corporate culture that will not permit any claim of wrongdoing.”).

102 See Geoffrey Miller, From Club to Market: The Evolving Role of Business Lawyers, 74 Fordham L. Rev. 1105, 1129 (2005) (“Clients that wish to test legal limits can select law firms that are willing to overlook problems. And because law firms need clients, they will face competitive pressures to offer lax supervision.”).

103 See, e.g., Richard W. Painter, Game Theoretic and Contractarian Paradigms in the Uneasy Relationship Between Regulators and Regulatory Lawyers, 65 Fordham L. Rev. 149, 170–71 (1996) [hereinafter Painter, Game Theoretic] (arguing that corporations can benefit from being represented by attorneys who have pledged or proven to regulators that they take monitoring obligations seriously); Richard W. Painter, Lawyers’ Rules, Auditors’ Rules and the Psychology of Concealment, 84 Minn. L. Rev. 1399, 1402–03 (2000) (“A client that wants a good relationship with investors, regulators and lenders may decide ex ante that secrets should not be kept by lawyers whom it hires to work on public offerings, mergers and similar transactions.”).
depend on the reputation for independence that the firm establishes with regulators in the field in which the firm practices.  

Whatever form of counsel is used, compliance-avoidance techniques are most likely to be found in corporations whose management is conscious of its own propensity for cutting corners. An attorney who is unwilling to play ball in such an organization will be unwelcome. Her choice not to use the committee alternative not only will be met with resistance, but also may be punished. In contrast, a well-socialized management team that wishes to be notified of potential law violations and hopes to meet a high standard of conduct will welcome a reporting lawyer’s initiatives. The alternative committee structure thus is unlikely to benefit companies that already are good citizens, or lawyers within them with information about wrongdoing.

C. Disclosure Rules

Disclosure rules are a third form of corporate blackmail. These rules present the extreme situation. A lawyer who exercises the right or obligation to disclose ordinarily knows that doing so will end any possibility of a future relationship with the client. External counsel will be dismissed. In-house counsel probably will be discharged, or at least isolated within the organization. The lawyer’s calculation of the personal costs inherent in exercising the blackmail option thus becomes inevitable.

Making the confidentiality exception discretionary has two effects. At least on the surface, it seems to allow the lawyer to include the potential personal costs in her calculus. And it allows lawyers to negotiate their blackmail threat without losing the moral high ground. In other words, a lawyer who threatens to disclose because an ethics rule says she must should not be able to be persuaded to forego disclosure on any basis other than that the client will correct the problem to the lawyer’s satisfaction. If the rule is discretionary, however, the lawyer arguably is authorized to accept a compromise solution, including one that benefits the corporate officers and herself.

Outside counsel can perhaps benefit most from these effects. Outside counsel typically are in a better negotiating position than in-house counsel, for several reasons. First, because they have less to lose—one client rather than their entire livelihoods—they have more

104 Painter, *Game Theoretic*, *supra* note 103, at 170–71 (arguing that law firms have a long-term interest in exhibiting law-abiding character to administrative agencies before which they practice).
leverage. Second, the relationship of retained, as opposed to salaried, lawyers almost always has started from an arms-length position of negotiation, one that both parties to the negotiation are conscious of. Third, the company is in a position to exact a range of retribution (all of which is negotiable) against a full-time employee, and so is more able to exert pressure for a favorable settlement. The discretionary nature of the disclosure exception thus does not necessarily make it more likely that outside counsel will disclose than in-house counsel, but it does make it more likely that outside counsel can use the option to benefit themselves or, at least, to produce some movement by the company on the moral issue.

When the disclosure exception is mandatory, disclosure will still cost the salaried employee more than the occasional outside counsel. But outside counsel’s ability to avoid responsibility (that is, to negotiate away the disclosure option) is less significant. In-house counsel, particularly one who is a low-level employee, may be able to share the responsibility with her supervisors and thus spread the costs of confronting management; the company is unlikely, for example, to discharge the whole legal staff. Moreover, if the lawyer has taken some steps, such as reporting part of the way up the ladder, enforcement agencies and plaintiffs’ lawyers are more likely to target the higher-ups, rather than the lower-level employees. The in-house lawyer thus has both great personal incentives to minimize her mandatory obligation and potentially greater ability to avoid sanctions if her failure to disclose is discovered. An outside law firm that has a clear obligation to disclose under the rules has lesser incentives to demur and will find it more difficult to escape punishment.

From the organization’s point of view, the above considerations cut in several directions. On the one hand, if a disclosure rule is permissive, it is easier for the company to manage the information provided to external counsel to avoid the possibility of a blackmail threat. On the other hand, once given the damaging information, in-house counsel is less likely to exercise the threat to disclose or to negotiate concessions for foregoing the blackmail option.105

The same calculus applies when the confidentiality exception is mandatory, except that the ability of the lawyers to negotiate and convince themselves that they have a legal or moral right to forgo disclosure disappears. The salaried employee’s costs of disclosure are higher

105 See Henning, supra note 21, at 327, 368 (noting that a mandatory withdrawal rule “may create a ‘race to the bottom’ by encouraging corporations to hire weak lawyers”).
than the external firm’s, but in foregoing disclosure the employee *knows* that she is doing something unethical and perhaps illegal. The external firm’s practical incentives to demur are slimmer.

State law regarding retaliatory discharge lawsuits for lawyers who are sanctioned for disclosing may affect the viability of the blackmail option. In most jurisdictions, external counsel would have a difficult time suing for retaliatory discharge in any event, because the common law rule is that clients should be able to retain only lawyers they trust. In some jurisdictions, the mandatory nature of disclosure may provide in-house counsel with a cause of action if she is discharged, which reduces her disincentives to employ coercion.\(^{106}\) Interestingly, however, at least one jurisdiction (i.e., Illinois) relies upon the mandatory nature of disclosure as a grounds for disallowing a retaliatory discharge cause of action,\(^{107}\) making in-house counsel in such jurisdictions less likely to follow the disclosure rule.\(^{108}\)

**D. Noisy Withdrawal Rules**

The fourth form of lawyer blackmail in the corporate context is noisy withdrawal. In large measure, threatening a noisy withdrawal is equivalent to threatening to disclose, because third parties ordinarily will be able to discern the reasons for the disavowal of prior representation. In some jurisdictions, however, the right to employ a noisy withdrawal is permissive, not mandatory, and is limited to situations in which the lawyer’s services have been used.\(^{109}\) When the lawyer simply

\(^{106}\) In Gen. Dynamics Corp. v. Super. Ct., 876 P.2d 487, 502–03 (Cal. 1994), for example, the California Supreme Court conditioned lawyers’ ability to sue for retaliatory discharge on the lawyer making only disclosures permitted under California’s attorney-client privilege standards.

\(^{107}\) In *Balla*, the Illinois Supreme Court reasoned that when a lawyer’s disclosure of information to protect third parties is required by the professional rules, there is no need to provide lawyers with an incentive to disclose through a retaliatory discharge cause of action. 584 N.E.2d at 108–09.

\(^{108}\) David Fish, *The Legal Rock and the Economic Hard Place: Remedies of Associate Attorneys Wrongfully Terminated for Refusing to Violate Ethical Rules*, 30 UWLA L. Rev. 61, 75 (1999) (arguing that cases like *Balla* underestimate counsel’s economic incentives to avoid disclosing their company’s misconduct); Justine Thompson, *Note, Who Is Right About Responsibility: An Application of Rights Talk to Balla v. Gambro, Inc. and General Dynamics Corp. v. Rose*, 44 DUKE L.J., 1020, 1043 (1995) (“By placing attorneys in this dilemma [of reporting at risk of being discharged], the *Balla* court discourages attorneys from making ethical choices consistent with community standards.”).

\(^{109}\) See *Model Rules of Prof’l Conduct* R. 1.6 cmt. (1983) (providing that Rules 1.6, 1.8, and 1.16 do not “prevent[1] the lawyer from giving notice of the fact of withdrawal, and the lawyer may also withdraw or disaffirm any opinion, document, affirmation, or the like”).
learns of corporate misconduct that has not involved her, she has no roving right to alert third parties.

This discretionary form of noisy withdrawal option essentially puts the lawyers in the same position as other corporate employees. They too have an obligation to keep the employer’s secrets, but not to the extent that silence would implicate them in a crime or fraud. The lawyer’s remedy is tied to the lawyer’s personal right to avoid the imputation of wrongdoing and liability for that wrongdoing. A rule allowing such conduct relieves counsel of ambiguity in other remedial rules that seem to forbid revelation of any corporate information.¹¹⁰

IV. WHEN SHOULD SOCIETY IMPOSE COERCIVE RESPONSIBILITY ON LAWYERS?

Perhaps the most interesting aspect of the above analysis is how little it has focused upon society’s actual interests in lawyer monitoring of corporate behavior and the countervailing interests in enabling clients to trust their lawyers. We have seen that different segments of the bar may favor or oppose coercive rules, or types of rules, for totally extraneous reasons. Some rules will lead companies to divert work from in-house counsel to external firms, and vice versa. Some rules allow companies to concentrate work in the hands of a few lawyers or firms, while others encourage companies to spread the work among multiple firms that engage in spot work. Some rules have uniquely deleterious effects on the day-to-day work life of staff counsel.

The discussion also has illustrated that different varieties of coercive authority may have effects on the conduct of companies that are perverse in light of the goals of providing such authority in the first place. Discretionary rules, for example, support the possibility of subtle negotiation between companies and lawyers about the lawyers’ threats, or willingness to make threats. It thus becomes likely that companies that wish to act lawfully and morally from the outset (and therefore need less heavy-handed monitoring) are more likely to engage lawyers who might exercise the blackmail option. Companies likely to cut corners will engage lawyers who are willing to negotiate away their power to enforce better conduct.

¹¹⁰ See Cal. Rules of Prof’l Conduct R. 3-600(C) (2004) (providing that if a client corporation persists in proposed wrongdoing despite the remedial steps the lawyer has taken, “the member’s response is limited to the member’s right, and, where appropriate, duty to resign”).
Alternative avenues of compliance, like QLCC’s\textsuperscript{111} or the actions of supervisory attorneys under the Sarbanes-Oxley regulations,\textsuperscript{112} similarly can be misused by those companies most willing to exert pressure on line attorneys to overlook misconduct. As we have seen, the initial reaction of corporations under Sarbanes-Oxley may be to limit information in the hands of each attorney and to disperse information to multiple outside firms.\textsuperscript{113} These firms often may not learn of corporate misconduct but, when they do, are capable of implementing the goals of the blackmail rules. To the extent a maverick company can establish a deferential QLCC, however, the calculus changes. The company will keep matters in-house and signal to staff attorneys that their jobs depend on their willingness to refer issues to the QLCC. In-house counsel can accede without personal liability or cost. The alternative compliance mechanism thus becomes a loophole.

Finally, as we have seen, actual implementation of coercive authority depends on an interplay between lawyers and companies that has little to do with the societal concerns underlying the rules. In-house counsel, external counsel who provide full service representation, and external counsel who perform spot work compete for business. Each has a different capacity to communicate with a company, negotiate in her own interests, and resist pressure to capitulate to management’s desires.\textsuperscript{114} In this competitive environment, companies will adjust their use of each type of lawyer in a way that minimizes the exercise of lawyer coercion.

All of this suggests that lawyer blackmail rules may have only limited effect on the ultimate lawfulness or morality of corporate behavior. Moreover, to the extent lawyers do try to control corporate conduct, it ultimately may be for self-serving reasons (for example, avoiding personal liability) rather than because lawyers wish to, or must, serve society’s goals. This leads to the core question: why would we authorize lawyers to force a client to follow their advice?

The automatic response of lawmakers who promoted regulations pursuant to the Sarbanes-Oxley Act is simply that lawyers have a role.

\textsuperscript{111} See 17 C.F.R. § 205.3(c) (2005).
\textsuperscript{112} See id. § 205.3(b).
\textsuperscript{113} See supra notes 46, 99 and accompanying text.
\textsuperscript{114} See Fisch & Rosen, supra note 8, at 1127–30 (noting that lawyers’ willingness to turn a blind eye to misconduct stems from their dependence on clients, but noting that this dependence may vary among different kinds of attorneys).
to play in preventing clients’ illegal acts before they occur. But some commentators expect lawyers to play a broader role—in preventing client fraud, legal but harmful acts, perhaps even immoral conduct, in addition to client illegality. For the most part, the existing codes draw a bright-line rule regarding illegal conduct: namely, that it is per se undesirable and that lawyers should never be allowed to countenance illegality, at pain of personal repercussions. But the codes seem ambivalent with respect to other forms of questionable client behavior to which attorney coercion might respond, including ill-defined breaches of fiduciary duty and poor business decisions. Lawyers traditionally have provided representation for clients involved in such behavior and society traditionally has condoned this representation. As a general principle, therefore, society may not be prepared to allow lawyers to make clients behave only in ways that the lawyers deem honest, fair, and moral.

Three broad considerations account for this reluctance. First, society probably does not trust lawyers to be the arbiters of honest, fair, or moral behavior, nor is there any reason to suspect that lawyers are well-suited to that task. Second, and related, is the fact that American society places a premium on individual autonomy. Clients have some right to make their own decisions regarding the fairness or morality of their conduct, though they may have to suffer the

115 See, e.g., Lisa H. Nicholson, Sarbox 307’s Impact on Subordinate In-House Counsel: Between a Rock and a Hard Place, 2004 Mich. St. L. Rev. 559, 589 (noting lawmakers’ view of the growing and important role of lawyers in the governance of issuers); Ahuja, supra note 8, at 1333 (noting the public interest in having attorneys report up the ladder); cf. Fred C. Zacharias, Reform or Professional Responsibility as Usual: Whither the Institutions of Regulation and Discipline?, 2003 U. Ill. L. Rev. 1505, 1511 n.30 (describing Sarbanes-Oxley as a response to the negative involvement of lawyers in recent corporate scandals).

116 Cf. Cramton et al., supra note 11, at 739 (praising the ABA’s stricter 2003 version of Model Rule 1.13 making reporting-up mandatory when that would be in the best interests of the organization); Report of the American Bar Association Task Force on Corporate Responsibility 39 (2003), available at http://www.abanet.org/buslaw/corporateresponsibility/final_report.pdf. (stating that communication up the corporate ladder “may be a desirable contribution to corporate governance even if the rules of professional conduct do not mandate it”).

117 See 17 C.F.R. § 205.2(i) (2005) (defining what lawyers need to report as evidence of a material violation, a material breach of fiduciary duty, or a similar material violation); Fisch & Rosen, supra note 8, at 1113–14 (suggesting that the “similar violation” language of Sarbanes-Oxley renders the provision too vague).

118 See Cal. Rules of Prof’l. Conduct R. 3-600(B) (2004) (requiring lawyers to act with respect to proposed corporate conduct that the lawyer believes is likely to injure the corporation).

119 See infra notes 122–126 and accompanying text.

120 See infra notes 127–128 and accompanying text.
consequences if their peers subsequently disagree with actions they have taken. Third, America’s litigiousness makes it imperative that clients be able to engage and confide in lawyers. Requiring lawyers to routinely turn against their clients might undermine the ability of clients as a whole to utilize lawyers.

A. Lawyers as Arbiters of Appropriate Conduct

One reason society may not be willing to give lawyers broad discretion to make clients behave in ways that the lawyer deems appropriate is that society probably does not trust lawyers to be arbiters of such behavior. If the recent corporate scandals make nothing else clear, it is that lawyers have not uniformly implemented the tools that they have had available to counteract corporate misconduct. Susan Koniak has made a persuasive factual presentation supporting the proposition that lawyers participated directly in some of the recent scandals. Even if one does not accept Koniak’s most flamboyant rhetoric, it is undisputable that at least some of the lawyers involved saw their main role as assisting clients to accomplish their ends, without making any moral judgments.

More important than this anecdotal evidence concerning the likely effectiveness of coercive rules, however, are two realities. First, there is no basis for thinking that most lawyers will act objectively to serve societal interests if simply given the opportunity to do so. That traditionally has not been the way lawyers have perceived their role. Lawyers are not trained in making moral judgments. Arguably, their education and practice requires them to view issues more in terms of competing arguments than appropriate results.

Second, as illustrated by this Article’s analysis, lawyers have personal incentives that sometimes prevent them from judging client conduct objectively. Far from possessing the definitional neutrality of members of the bench, lawyers are naturally aligned with clients. The business reasons for which lawyers ordinarily enter the attorney-client relationship suggest that they will emphasize economic rather than outward-regarding considerations.

121 See infra notes 129–138 and accompanying text.
122 Koniak, supra note 75, at 196–211; see Partnoy, supra note 8, at 331 (documenting the actions of counsel in the Enron scandal); Pugh, supra note 39, at 662–64 (discussing the role of lawyers in the Enron scandal).
These realities have implications for coercive rules. They explain the hesitation of some code drafters to rely on lawyers to do more than counsel against illegal conduct. They also illustrate why reforms that purport to enhance lawyer authority to force appropriate client conduct may not do the trick.

Discretionary rules, like new Model Rules 1.6 and 1.13, may not adequately confront lawyers’ natural limitations. To justify making lawyer gatekeeping optional, rulemakers need some special reason to set aside the traditional distrust of lawyers. As this Article’s analysis suggests, the corporate setting that has stimulated recent reforms does not look like a promising context for outward-regarding lawyer behavior.

Reformers also have done a questionable job of confronting the way coercive rules will operate in practice. Given the fluid nature of the attorney-client relationship described in this Article, coercive rules should be written with sufficient precision to ensure that coercive authority works in its intended fashion. Specifically, they should include safeguards to prevent lawyers from avoiding the obligation to implement coercion impartially. In other words, the drafters must take a realistic view of the economics of practice in determining whether lawyers will exercise their options with a view to the drafters’ purposes. The drafters also may need to make distinctions in the rules that take into account the incentives of different types of lawyers. On this view, even the mandatory SEC requirements seem to fall short.

B. Client Autonomy

The premium society places on client autonomy is a second consideration that might caution against giving lawyers broad coercive power. In the corporate context, however, autonomy considerations do not have the same force as when individuals’ freedom to select

---

124 Cf. McGowan, supra note 12, at 1838 (proposing and analyzing a systematic grant of immunity from liability to lawyers that would provide incentives for them to inform authorities about corporate illegality).

125 See Fred C. Zacharias, The Future Structure and Regulation of Law Practice: Confronting Lies, Fictions, and False Paradigms in Legal Ethics Regulation, 44 Ariz. L. Rev. 829, 841 (2002) (characterizing the ethics codes’ general assumption that all lawyers are alike and should be governed by the same rules as counterproductive); Fred C. Zacharias, Reconceptualizing Ethical Roles, 65 Geo. Wash. L. Rev. 169, 171 (1997) (arguing that ethics codes should acknowledge differences among types of lawyers).

126 See, e.g., Cramton et al., supra note 11, at 751–63 (arguing that the trigger mechanisms in the Sarbanes-Oxley regulations allow lawyers too much leeway); Koniak, supra note 76, at 1275–78 (questioning the effectiveness of SEC regulations governing lawyers).
conduct is at issue. Corporations have economic rights, which benefit all their constituents, but their constituents typically are sufficiently diverse that they would disagree on most moral issues. Preserving the authority of one corporate agent to act autonomously may well deprive other constituents of the same freedom.

Thus, to the extent professional norms require lawyers to abide by corporate clients’ decisions, they are not rejecting principles of autonomy so much as deciding who within a corporation is most likely to exercise the corporation’s ability to make choices that best accommodate the firm’s economic interests and society’s separate interest in appropriate outward-regarding conduct. Rules that limit lawyers’ ability to force behavior make one of two judgments (or both). First, they may assume that lawyers usually are not in the best position to balance the interests—for example, because lawyers will have limited information about the grand scheme in which a case arises or because lawyers have limited economic or moral expertise in implementing the necessary calculus. Second, the rules may simply assume that the lawyers in question are unlikely to implement societal interests any better than management. As we have already seen, in-house counsel often are too tied or dependent on management to challenge management’s decisions. External counsel may focus too heavily on their own interests in earning present and future fees.

Rules that allow or require lawyers to influence corporate clients’ conduct also may stem from a variety of justifications. Most, but not all, such rules confine themselves to addressing illegal client behavior. Because lawyers are versed in the law, they arguably have special expertise in determining what conduct is appropriate and permissible.

It is important to recognize the limits of this reasoning, however. In most blackmail situations, there is little question about the legality of the conduct itself. Even if there is, the lawyer can eliminate the

---

127 There are exceptions, however. California’s professional rules, for example, arguably require lawyers to act against economically imprudent corporate decisions. See CAL. RULES OF PROF’L CONDUCT R. 3-600(B) (2004); supra note 52 and accompanying text. The Sarbanes-Oxley regulations require lawyers to counteract “material violations” of securities obligations or “breaches of fiduciary duty” by an issuer. 17 C.F.R. §§ 205.2(i), 205.3(b) (2005) (requiring lawyers to report a material violation, defined as a material violation under federal or state securities laws, a “material breach of fiduciary duty,” or a “similar material violation” of any federal or state law). Other administrative regulations impose responsibility on lawyers to supersede their clients’ decisions to file information that is arguably accurate but misleading. See Fred C. Zacharias, Understanding Recent Trends in Federal Regulation of Lawyers, 2003 Prof. Law. 15, 16–21 (cataloguing some of these regulations).
question by providing legal advice. The real issue—for example, in Enron—is whether the client should, or should be able to choose to, violate the law. On this, the lawyer has no more expertise than the corporate manager. Accordingly, the reason for placing the decision in the lawyer’s hands must be something else.

Perhaps the reason consists of a sense that lawyers are more likely to act independently or objectively than the managers, or more in the interests of the silent corporate constituents. As this Article has discussed, however, one cannot assume independence on the part of the lawyer in all circumstances. In-house counsel, in particular, may have as much to lose from insisting on lawful conduct as the corporate manager. If the governing rule has the effect of influencing corporations to spread legal work among many different external firms, the rule may in fact generate a body of relatively independent lawyer decision makers. At the same time, however, these lawyer decision makers are also likely to be given less than the optimal amount of information to make decisions.128

C. Facilitating or Enabling the Provision of Legal Advice

Society’s reluctance to overemphasize lawyers’ ability to coerce clients may be attributable to a fear of undermining the traditional attorney-client relationship. On one level, coercive regulation—particularly mandatory blackmail rules—simply clarifies ambiguity created by previous ethics regulation that seems to require lawyers to assist corporate clients and remain silent about potential wrongdoing. Lawyers are accountable for their own actions. When they participate in unlawful or tortious conduct, they can be sanctioned.129 Authorizing lawyers to counteract the wrongful conduct arguably makes explicit the notion that legal representation does not include enlisting a lawyer as a co-conspirator.130

128 See supra note 46 and accompanying text.
129 See Zacharias, supra note 13, at 1396, 1396 nn.51–55 (listing authorities that describe ways in which lawyers can be sanctioned for participating in unlawful conduct).
130 George Cohen perhaps best encapsulates the regulatory balance that needs to be struck between confidentiality requirements and disclosure exceptions:

Although clients benefit from confidentiality rules, and the attorney-client privilege and work product doctrine give lawyers market advantages over other groups, these benefits come at a price, namely, the limitations designed to thwart lawyer-client collusion. You have to take the bad with the good. For this to work, however, the “good” has to be good enough for clients and lawyers to buy into the system.
This perspective helps explain those rules that authorize disclosure or noisy withdrawal with respect to aspects of corporate misconduct in which a lawyer’s services have been used.\textsuperscript{131} It does not, however, justify broader rules that expect lawyers to counteract client wrongdoing in which they have not participated.\textsuperscript{132} This distinction highlights the quandary raised by the whole notion of a blackmail option; namely, the extent to which society wants lawyers to act as a unilateral check on client misconduct.

When one views the adversarial system fairly, it is clear that our legal system does not contemplate lawyers routinely policing their clients, because that would lead to the avoidance of legal representation or increased use of lawyers who have reputations for disregarding their professional obligations. The core notion of the system is that we want clients to use and trust legitimate lawyers so that the lawyers can do their jobs and enable the system to accomplish its functions.\textsuperscript{133}

Society does have an interest in having clients consult lawyers about legal issues and receive advice regarding the lawfulness of their conduct. Arguably, society may even be willing to insist that clients follow that advice to the extent that it identifies actions that clients must avoid to satisfy the law. On the surface, however, the interest in promoting law-abiding behavior cuts against rules that would allow lawyers to threaten clients into acting morally or into avoiding wrongful actions for which there is a legitimate argument in favor of their lawfulness.\textsuperscript{134} Clients are unlikely to confide in a lawyer whom they know can force them to abide by her personal moral code.

\textsuperscript{131} E.g., Model Rules of Prof’l Conduct R. 1.6(b)(2)–(3) (2002); 17 C.F.R. § 205.3(d)(2); Proposed SEC Noisy Withdrawal Rule, supra note 11, at 71,706, quoted in 68 Fed. Reg. 6324, 6326 (allowing lawyer to disaffirm false or misleading filings “that the attorney has prepared or assisted in preparing”).

\textsuperscript{132} Cal. Rules of Prof’l Conduct R. 3-600(B) (containing no requirement of lawyer participation in the wrongdoing before lawyer permitted to act).

\textsuperscript{133} See, e.g., David Luban, Lawyers and Justice 68–81 (1988) (discussing the consequentialist justifications for the adversary system); Fred C. Zacharias, Structuring the Ethics of Prosecutorial Trial Practice: Can Prosecutors Do Justice?, 44 Vand. L. Rev. 45, 46–56 (1991) (outlining the theoretical underpinnings of the adversary system); cf. Freedman & Smith, supra note 16, at 13–43 (discussing the theory of the adversary system, but also emphasizing client autonomy considerations).

\textsuperscript{134} Compare 17 C.F.R. § 205.3(d)(2) (2005) (allowing attorneys to report confidential information that the attorney reasonably believes is necessary to prevent the issuer from committing a material violation), with id. § 205.3(b)(6)–(7) (absolving some investigating attorneys from reporting under some circumstances when “retained or directed . . . to
It is the bright-line nature of these conclusions that highlights the real difficulty inherent in assuming lawyers have more than an advisory role in counteracting client misconduct. Is there illegal client conduct that a lawyer sometimes should countenance? Some commentators might answer affirmatively with respect to at least three scenarios: lawyers arguably should defer to the client (1) because (or when) coercion would unduly deter this and other clients from seeking legal advice on other issues in the future; (2) when a client, such as the corporation, is acting reasonably by violating the law—for example, because the benefits of non-compliance outweigh the costs; and (3) when it is too late for the lawyer to stop the violation of law, or the costs to the client of stopping it at this stage are draconian compared to the benefits to society of full law compliance.

Conversely, is there legal but otherwise inappropriate behavior regarding which a lawyer should unilaterally be able to countermand the client’s autonomy? In the corporate context, one can skirt the issue somewhat by concluding that certain corporate decision makers sometimes are not exercising the client’s autonomy—in other words, are not actually acting in the corporation’s interests. More generally, one might conclude that some societal or third-party interests simply are more important than the client’s interest in controlling the decision and achieving the result most beneficial to the client.

The problem for rulemakers is that it is hard to draw clear lines that balance society’s interest in law compliance or “good results” against the other interests. Consequently, most rules that acknowledge the possibility of grey areas use one of two proxies. Some limit a lawyer’s options to situations in which the lawyer’s actions are “in the interests of the organization,” which does not adequately take into account society’s interests in behavior that affects the public or third parties. Other rules simply give lawyers discretion to act, which al-

---

135 Arguably, lawyers always have the authority to advise clients to act morally or in a socially acceptable way, and professional rules could impose an obligation on lawyers to do so always. * Cf. Model Rules of Prof’l Conduct R. 2.1 (2002) (authorizing lawyers to counsel clients regarding moral and political issues).

136 Model Rules of Prof’l Conduct R. 1.13(b) (2002); * cf. 17 C.F.R. § 205.5(d) (allowing lawyers to make disclosures to prevent injury to the property of the issuer or investors).

137 Model Rules of Prof’l Conduct R. 1.6(b) (2002). It may be that rules that refer to lawyers’ ability to exercise discretion intend discretion to be exercised in a particular way. * Compare Samuel J. Levine, * Taking Ethical Discretion Seriously: Ethical Deliberation as Ethical Obligation*, 37 Ind. L. Rev. 21, 46 (2003) (arguing that discretion must be exercised in a
allows lawyers to base their decisions on personal, potentially venal, incentives. A discretionary rule may be the best solution, but the interests to be balanced should be better defined if the goal is to use lawyers as a surrogate enforcer of societal interests.

Consider, for example, the old version of Model Rule 1.13, which requires lawyers to act but gives them the choice of remedy. The rule requires lawyers to act in the “organization’s interest,” which presumably allows counsel to consider countervailing costs to the company. The rule, however, does not tell lawyers how to weigh those costs, or even directly to emphasize them. It thus opens the door to pressure from management.

Now consider the Sarbanes-Oxley regulations, which make it mandatory for lawyers to climb the ladder with concerns about illegal conduct or breaches of fiduciary duty. These rules do not allow lawyers even to consider the effect of climbing the ladder on the institution’s willingness or ability to consult counsel.

The discretionary disclosure provisions of new Model Rule 1.13 allow lawyers to disclose (or threaten to disclose) specifically in circumstances in which illegal corporate activity “is reasonably certain to result in substantial injury to the organization.” By limiting its scope to illegal conduct, Rule 1.13 is drawing a defensible bright-line rule: corporate clients have no right to insist on breaking the law. At first glance, the rule also seems to inform the lawyer of how to balance the corporation’s interest in confessing its conduct when doing so will be economically damaging—disclosure is only appropriate when the organization will suffer substantial injury as a result of the illegal conduct. Yet upon closer examination, because any illegality is likely to cause substantial injury if the client is caught and sanctioned, the rule falls short. It again fails to guide lawyers on how to act when the net balance of the injury versus the potential economic gain of maintaining silence favors silence. By leaving the issue entirely to lawyer discretion—indeed, by not even noting the possibility that the substantial injury will be outweighed—the rule allows lawyers to exer-

deliberative fashion), with McGowan, supra note 12, at 1825 n.1 (arguing that a grant of discretion means that a lawyer may not be disciplined for acting in any manner she sees fit). This issue probably is too complex to resolve uniformly with respect to all discretionary rules because code drafters may have a variety of reasons for according lawyers a range of options. See generally Bruce A. Green & Fred C. Zacharias, Lawyer Discretion, 91 MINN. L. REV. (forthcoming 2006) (discussing the justifications for discretionary rules).

exercise their discretion without reference to the reasons why society might want lawyers to act in a particular direction.

V. Other Blackmail Contexts

Much of the recent controversy concerning potential attorney coercion has focused on corporate attorneys and rules like Model Rule 1.13 and the Sarbanes-Oxley regulations. Interestingly, however, these rules actually are relatively well-defined—at least when compared to rules that allow lawyers to coerce clients to accept the lawyers’ will in other contexts. Most of the rules governing organizations at least focus directly on breaches of legal duties, which lawyers arguably should not countenance and already are forbidden to assist.139

Consider a few other forms of attorney coercion, however. Typically, lawyers are authorized to resign from representation when a client wishes to pursue avenues the lawyer considers “repugnant,” “imprudent,” or with which the lawyer has “fundamental disagreement.” At one level, the threat to withdraw hardly seems coercive. The client still has the option to retain other counsel who is willing to do as the client wishes. But often, hiring new counsel will be expensive, cause delay, and may be emotionally difficult for clients—especially individual clients who are unfamiliar or uncomfortable with the process of retaining counsel. Moreover, in some situations, allowing a lawyer to withdraw simply is unrealistic—for example, when a lawyer insists that the client accept a settlement which is close to what the client would otherwise accept, but is not quite at that level. Substituting counsel at this juncture may cause the offer to be reduced, because the adversary will know that the client’s costs of proceeding have risen.

What is distinctive about coercion through threatened resignation is that it need not be based, like the lawyer action under the organizational rules, on proposed illegality by the client. The lawyer may make her threat simply because she disagrees strongly with the client’s view—as a moral matter or as one of legal strategy. The resignation power thus gives lawyers broad discretion to impose their will on malleable clients.

---

139 See id. at R. 1.2(d) (“A lawyer shall not . . . assist a client in conduct that the lawyer knows is criminal or fraudulent.”).
140 Id. at R. 1.16(b) (4).
In exercising this discretion, lawyers presumably have the capacity to consider their personal economic interests; in other words, the extent to which they are prepared to risk their fees and the extent to which their own interests are benefited by client compliance with their directions. Lawyers also have broad leeway to emphasize moral considerations, even though that cuts directly against the notion of client autonomy. Presumably, the codes intend lawyers to restrain their own use of coercion, because lawyers continue to be bound by fiduciary duties to clients and the bar’s tradition of honoring client decision making, but nothing in the rules emphasizes those limitations.\textsuperscript{143}

By the same token, the more that lawyers are known to use their resignation power to control distasteful clients, the less clients will allow lawyers to learn about them. The traditional paradigm is that clients should feel free to confide information that may not bear directly on the legal issues at hand, leaving it to counsel to determine what is useful.\textsuperscript{144} In the criminal defense context, in particular, clients may be hesitant to reveal facts that make them seem “repugnant”—including facts about past criminality, ongoing sexual proclivities, and other vices. One would expect two dynamics to result from lawyers’ coercive use of this information: (1) more clients—especially those who are most conversant with lawyers’ actual practices—will self-censor, and (2) a market will develop of lawyers with a reputation for not exercising coercion.

The withdrawal power is not the only instance in which lawyers can force clients to accede to their will. The codes, for example, give lawyers discretion not to introduce evidence they believe to be false.\textsuperscript{145} By threatening not to put a client on the stand, a lawyer can coerce the client into agreeing to testify in the way the lawyer deems acceptable.\textsuperscript{146}

More broadly, a lawyer can use her authority to determine the tactics in a case to force a client to adopt an approach to the case that is not in


\textsuperscript{144} This is the justification for the broad definition of confidential information that is found in all the professional codes. The Model Rules, for example, define confidential information as all information “related to the representation.” Model Rules of Prof’l Conduct R. 1.6(a) (2002). The Model Code incorporates all “information gained in the professional relationship.” Model Code of Prof’l Responsibility DR 4-101(a) (1969).

\textsuperscript{145} Model Rules of Prof’l Conduct R. 3.3 (1983) (stating that “[a] lawyer may refuse to offer evidence that the lawyer reasonably believes is false”).

line with the client’s desires.\(^\text{147}\) Thus, for example, a client might prefer a scorched earth approach or aggressive cross-examination of tender witnesses, but the lawyer may—by threatening to withhold harsh cross-examinations—prevail upon the client to accept a different theory of the case that cedes some substantive positions the client could otherwise insist upon taking.\(^\text{148}\)

In all of these situations, as well as situations in which lawyers are granted discretion to disclose confidential information in order to preserve third-party interests,\(^\text{149}\) the power to blackmail clients is far broader than the power identified in organizational rules. It is not limited to illegal choices the client might make, nor limited (at least not ostensibly) in the grounds upon which the power may be exercised. As a practical matter, lawyers therefore can use their authority to insist upon client decisions that the lawyers consider morally required, but that the clients do not. Lawyers also have leeway to take their own economic incentives into account, as in the corporate setting. Although this leeway theoretically is constrained by fiduciary principles, the rules themselves do not specify when and how the discretion to blackmail may be exercised. The codes, in short, leave it to individual lawyers to balance the societal concerns regarding client autonomy and facilitation of legal representation without directly attempting to assure that lawyers act upon those considerations.

In general, it is individual clients who will be most prone to lawyer blackmail. Three characteristics would make a client especially prone to coercion. Clients least familiar with the process of obtaining new counsel and with the alternative representation that may be available are most likely to accede to the lawyer’s threats. Those who are

\(^{147}\) **Model Rules of Prof’l Conduct** R. 1.2(a) (1983) (assigning lawyers authority to determine the means of litigation). The new Model Rules are somewhat less clear on this issue, noting that usually the client will defer to the lawyer on questions of tactics, but leaving unstated who controls the decision if the lawyer and client ultimately disagree. See **Model Rules of Prof’l Conduct** R. 1.2 cmt. (2002).

\(^{148}\) The dynamic effect of attorney blackmail may become most evident when lawyers assert coercive power by inferring authority from imprecise rules. In *Nix v. Whiteside*, for example, a lawyer confronted by potential client perjury not only threatened to inform the court, but also threatened to impeach the client if he took the stand and testified to a particular story. 475 U.S. 157, 161 (1986). The U.S. Supreme Court apparently approved this process—which starkly changed the participants’ relative power status within the attorney-client relationship. See *id.* at 168–69 (noting the “special duty of an attorney to prevent and disclose frauds”). After the lawyer’s threats, one can reasonably assume that the client would let the lawyer call the future shots, but also would revise his trust in and use of counsel.

\(^{149}\) **Model Rules of Prof’l Conduct** R. 1.6(b) (2002) (permitting disclosure to prevent harm to the financial interests or property of another).
limited by cost considerations also are vulnerable; it is the smaller cases in which lawyers will be most willing to chance their fees. Finally, clients who already know that a court will not allow them to discharge a lawyer (for example, because discharge has already been attempted) have the least ability to resist a threat.

When these characteristics are considered together, it appears that it is the poorest and least sophisticated clients whose autonomy is most likely to be restricted by lawyer blackmail. Yet it is precisely the autonomy of these kinds of clients that the rules, and the adversarial ethic they embody, are supposedly designed to protect.150 By failing to include guidelines or protections for client interests in the terms of blackmail rules, the code drafters may take with one hand what they have purported to give with the other.

This Article would be remiss if it did not address, albeit briefly, the most common form of lawyer coercion—psychological pressure imposed by forceful lawyers giving clients (especially dependent clients) advice in a result-oriented fashion. The theory of the professional codes is that clients should set the objectives of representation and that lawyers should enhance client autonomy.151 But the codes also encourage lawyers to exercise independent judgment, remonstrate with clients, and counsel them based on a variety of factors other than the client’s immediate desires.152 As a matter of practice, everyone knows that lawyers often use this authority to persuade or bully clients into making decisions—particularly plea and settlement decisions—that the lawyers consider appropriate.

Presumably, lying to a client in order to produce his agreement would not be countenanced by disciplinary authorities or by courts enforcing fiduciary principles. Suppose, however, that a lawyer simply is forceful. Or suppose that the lawyer uses her authority to withhold information temporarily from a client153 so that she can present the

150 See Zacharias, supra note 27, at 169, 171, 173–74 (discussing the “criminal paradigm” and its civil parallels).
151 See Model Rules of Prof’l Conduct R. 1.2(a) (2002) (stating that “a lawyer shall abide by a client’s decisions concerning the objectives of representation”).
152 See id. at R. 2.1 (stating that “a lawyer shall exercise independent professional judgment and render candid advice”). See generally Zacharias, supra note 123 (discussing the role of objectivity in legal practice).
153 See, e.g., Model Rules of Prof’l Conduct R. 1.4 cmt. (2002) (stating that “the lawyer should fulfill reasonable client expectations for information consistent with the duty to act in the client’s best interests”); cf. id. at R. 1.2 cmt. (noting that “[i]n a case in which the client appears to be suffering diminished capacity, the lawyer’s duty to abide by the client’s decisions is to be guided by reference to Rule 1.14”).
options at a time when the client will be more malleable.\textsuperscript{154} In theory, client autonomy remains intact because the client is the ultimate decision maker. Yet the lawyer is in control.

It is important to note that the lawyer’s action in these scenarios may or may not be in the client’s best interests. Consider, for example, the lawyer who forcefully convinces an innocent criminal defendant to plead guilty on the (realistic) basis that conviction is likely. Or consider the lawyer who persuades a client who insists that he is sane to pursue an insanity defense.\textsuperscript{155} One can argue both that the lawyer is serving the client’s interests and that the lawyer deprives the client of true autonomy.

For purposes of this Article, we need not resolve these troubling issues. The essential point is that lawyer coercion, for whatever reason, is routine. In some of the cases in which clients might have personal reasons for pursuing one course of conduct, their lawyers may have personal reasons for pursuing another—for example, because lawyers prefer saving a client to letting the client have his day in court.\textsuperscript{156} Furthermore, the rules that give lawyers discretion, or even more poignantly encourage lawyers, to advise clients coercively are most powerful with respect to clients who are poor (and thus unable to change lawyers), unsophisticated, and dependent. The professional codes themselves do little to guide lawyers on how they must exercise coercive authority, nor do the codes reconcile that authority with the codes’ broader theories of representation.

\textsuperscript{154} The classic example is when a criminal defendant forbids the lawyer even to discuss a plea bargain, but the lawyer nonetheless obtains a plea offer and waits to offer it to the client until the eve of trial, when fear of conviction is likely to make the client more receptive to admitting guilt.

\textsuperscript{155} In the Unabomber case, for example, Theodore Kaczynski’s lawyers went to great lengths to preserve the option of an insanity plea or the ability to present evidence of mental instability during the guilt phase of trial despite Kaczynski’s direct order that they not pursue that course. United States v. Kaczynski, 239 F.3d 1108, 1111–12 (9th Cir. 2001); id. at 1119, 1122 (Reinhardt, J., dissenting); see also H. Richard Uviller, \textit{Calling the Shots: The Allocation of Choice Between the Accused and Counsel in the Defense of a Criminal Case}, 52 Rutgers L. Rev. 719, 729–37 (2000) (discussing the Unabomber case). In so doing, they may have saved his life.

\textsuperscript{156} \textit{Cf.} Langevoort & Rasmussen, \textit{supra} note 44, at 375 (stating that “little if any serious attention has been given to the possibility that self-serving behavior will occur consciously or unconsciously in one of the most basic of the lawyer’s roles, that of giving legal advice to a client” and noting that lawyers may tend to overstate legal risk).
CONCLUSION

The assumptions underlying the organizational blackmail rules are that the rules will force lawyers to promote lawful behavior by corporate clients. The assumption of the more general coercive provisions in the professional codes is that lawyers will use their power to temper the exercise of client autonomy by encouraging moral decision making by clients. This Article’s analysis of the rules and lawyers’ incentives in implementing the rules, however, suggests that the reality is likely to be far more fluid.157 Lawyers have their own interests in the exercise of coercive authority that may be inconsistent with, or undermine, the code drafters’ intent. At least sophisticated clients will adjust their behavior to mitigate the lawyer’s power over clients that blackmail rules provide.

The existence of these dynamics also suggests that lawyers may promote or support the adoption of some coercive rules for reasons that do not align with the rules’ substantive justifications. Each possible phrasing of the organizational blackmail provisions will benefit one segment of the corporate bar over another. With respect to the more general rules governing coercive authority of lawyers, most lawyers’ personal interests align in favor of discretionary provisions that provide them with leeway to emphasize personal concerns. This consensus, in part, helps explain the relative sparseness in the rule drafting process of consideration of guidelines or specific limits on the exercise of discretion.158

Consider this question: may a law firm, in its retainer agreement, cede its discretion to disclose confidential information under a confidentiality exception in exchange for a higher fee? Most professional responsibility academics would answer in the negative, arguing that the discretion must at least be exercised and that it should be exercised in light of the public-regarding considerations that the codes clearly intend to emphasize.159 Some private lawyers, however, would

---

157 See Kim, supra note 92, at 1037 (arguing that “the ethical ecology is . . . complex,” that “[i]nside counsel are subject to situational pressures arising out of their multiple roles as mere employees, faithful agents, and team players,” and that “Sarbanes-Oxley does nothing to mitigate those pressures”).

158 Even if lawyers do not overtly sell their authority to disclose for a higher fee, firms can produce the same result by developing a reputation for serving as ultra-aggressive client-centered lawyers.

159 See, e.g., Levine, supra note 137, at 46 (proposing a deliberative model of exercising professional discretion); Fred C. Zacharias & Bruce A. Green, Reconceptualizing Advocacy Ethics, 74 GEO. WASH. L. REV. 1, 54 (2005) (discussing the obligation of lawyers to in fact exercise discretion); Green & Zacharias, supra note 137 (discussing the significance of
disagree and would view the rules simply as giving a “right” to lawyers that they may exercise in their own interests if they see fit to do so. Particular kinds of lawyers, and lawyers with particular attitudes towards legal practice, can benefit more than others from this characterization of discretion.

Because client autonomy concerns and the desire to encourage clients to trust and use lawyers are fundamental principles on which the professional codes are based, the failure to define lawyers’ coercive authority is anomalous. The failure of the drafting process to contemplate definitions can, perhaps, be explained on public choice grounds—that lawyers, as an interest group, have hijacked the drafting process away from serious consideration of the rules’ effects and of the way lawyers are likely to implement them. Future debates on such rules should rely less on platitudes concerning the societal interests at stake and more on how those interests are likely to be served.

discretionary rules). Other academics, such as my colleague David McGowan, might conclude that lawyers could (or would) not be disciplined for failure to exercise their discretion to disclose, but might be bound by fiduciary principles to implement the rules in the best interests of their clients. See McGowan, supra note 12, at 1827 (arguing that permissive disclosure rules allow lawyers not to disclose without cost to themselves, leaving them to decide whether disclosure will create costs).

160 See McGowan, supra note 12, at 1825 n.1 (suggesting that there is no obligation of lawyers to exercise discretion in a particular way, or even to exercise discretion). The drafters of the new California future crime confidentiality exception have provided fodder for proponents of the proposition that grants of discretion to lawyers are absolute by including a provision that lawyers may never be deemed to have violated the rule by failing to disclose and at the same time adding a comment stating that lawyers are not subject to discipline for revealing information pursuant to the rule. Cal. Rules of Prof’l Conduct R. 3-100(E) & discussion ¶ 5 (2004).
Abstract: Information to, from, and about U.S. persons routinely comes into the possession of the National Security Agency (the “NSA”) through the lawful warrantless surveillance of foreign persons abroad. The NSA’s internal administrative guidelines allow such information to be disseminated to law enforcement if it evinces any criminal conduct on the part of the U.S. person. This information may therefore be used to initiate domestic criminal investigations against U.S. citizens and other protected persons despite the fact that no warrant authorized the initial surveillance. The NSA’s guidelines contain no qualification as to the type of criminal offense that may be revealed, and no consideration of the individual’s reasonable expectation of privacy. Using encrypted Internet telephony as an example, this Article proposes a change to the NSA’s internal guidelines that would prevent dissemination of information gained through the frustration of the reasonable privacy expectations of protected persons unless exigent circumstances or serious threats to national security were presented.
The warrant clause of the Fourth Amendment is not dead language. . . .  
“It is not an inconvenience to be somehow ‘weighed’ against the claims of police efficiency. It is, or should be, an important working part of our machinery of government, operating as a matter of course to check the ‘well-intentioned but mistakenly over-zealous executive officers’ who are a part of any system of law enforcement.”

—United States v. U.S. Dist. Court (Keith) (Powell, J.)

INTRODUCTION

On December 16, 2005, the New York Times published a front-page story revealing the existence of a secret executive order issued by President George W. Bush in the months following the September 11, 2001 terrorist attacks on the United States. According to the article, the executive order authorizes the National Security Agency (the “NSA”) to conduct electronic surveillance on U.S. citizens and permanent residents inside the United States without first obtaining a warrant from the Foreign Intelligence Surveillance Court as mandated by the Foreign Intelligence Surveillance Act of 1978 (“FISA”). This appears to be a stark departure from the law governing domestic surveillance, and it raises serious constitutional questions about the limits of presidential power in times following national emergencies.

The current situation is returning FISA to the spotlight, and many of the Act’s more controversial provisions are being reexamined. FISA was passed in order to provide the executive branch with a quick and secure means of satisfying the Fourth Amendment’s warrant requirement for domestic investigations related to foreign intelligence and counterterrorism. The Act primarily controls the government’s surveillance of domestic communications involving U.S. without a court order and concluding that courts likely will find the program to be inconsistent with federal law); Letter from Curtis A. Bradley, Richard & Marcy Horvitz Professor of Law, Duke Univ., et al., to the Honorable Bill Frist, Majority Leader, U.S. Senate, et al. (Jan. 9, 2006), available at http://www.cdt.org/security/20060109legalexpertsanalysis.pdf (concluding that President Bush’s executive order is unlawful); see also FISA, 50 U.S.C. § 1809(a) (2000) (“A person is guilty of an offense if he intentionally engages in electronic surveillance under color of law except as authorized by statute . . . .”); Authorization for Use of Military Force, Pub. L. No. 107-40, 115 Stat. 224 (2001) (codified at 50 U.S.C. § 1541 note (2000 & Supp. III 2003)) (“[T]he President is authorized to use all necessary and appropriate force against those nations, organizations, or persons he determines planned, authorized, committed, or aided the terrorist attacks that occurred on September 11, 2001, or harbored such organizations or persons, in order to prevent any future acts of international terrorism against the United States by such nations, organizations, or persons.”) (emphasis added); Keith, 407 U.S. at 321 (reasoning that the CIA may not conduct domestic surveillance for national security purposes without a warrant); Katz v. United States, 389 U.S. 347, 357 (1967) (“Over and again this Court has emphasized that the mandate of the [Fourth] Amendment requires adherence to judicial processes,’ and that searches conducted outside the judicial process, without prior approval by judge or magistrate, are per se unreasonable under the Fourth Amendment . . . .”) (quoting United States v. Jeffers, 342 U.S. 48, 51 (1951) (citation omitted)); Youngstown Sheet & Tube Co. v. Sawyer (Steel Seizure), 343 U.S. 579, 637 (1952) (Jackson, J., concurring) (reasoning that the President’s authority to protect national security is at its lowest ebb whenever the President seeks to act in violation of an act of Congress); Tom Daschle, Editorial, Power We Didn’t Grant, Wash. Post, Dec. 23, 2005, at A21 (stating that not only did Congress not intend the Authorization for Use of Military Force (the “AUMF”) to allow warrantless surveillance within the United States, but also that such broad domestic authority was specifically requested prior to the AUMF’s passage and that request was denied).

6 See Mark Moller, Untwist the Chain of Command, LEGAL TIMES, Feb. 28, 2006, available at http://www.law.com/jsp/dc/PubArticleDC.jsp?id=1141047297225 (detailing various perspectives on the procedural framework established under FISA); see also Jerry Crimmins, NSA Wiretaps Debated at U of Chicago, CHI. DAILY L. BULL., Feb. 1, 2006, at 1 (detailing a discussion held at the University of Chicago Law School between University of Chicago Law Professor Geoffrey R. Stone and Seventh Circuit Judge Richard A. Posner regarding warrantless NSA surveillance and the efficacy of FISA’s provisions); Patricia Manson, Bar Group to Debate Curbs on Federal Surveillance Activities, CHI. DAILY L. BULL., Feb. 10, 2006, at 1 (stating that U.S. Representative Heather Wilson, R-N.M., had called for a full review of the NSA warrantless domestic surveillance program and mentioning the possibility of new legislation that would amend FISA’s provisions).

7 S. REP. NO. 95-604, at 15 (1977); see also Susan Goering, An Unnecessary Breach of Law, BALT. SUN, Dec. 21, 2005, at 19A (discussing the compliant nature of the Foreign Intelligence Surveillance Court, and stating that out of the 18,747 warrant petitions received by the court from 1979 to 2005, only four were rejected).
citizens or permanent residents;\textsuperscript{8} it does not limit electronic surveillance of any communications between aliens outside the United States.\textsuperscript{9} The NSA may freely surveil such conversations with virtually no limitations under U.S. law.\textsuperscript{10}

FISA maintains a strict distinction between purely domestic calls between U.S. persons, and purely foreign communications between non-U.S. persons outside the United States.\textsuperscript{11} Surveillance of the former always requires approval from the Foreign Intelligence Surveillance Court, whereas surveillance of the latter never requires such approval.\textsuperscript{12} A substantial gray area exists when calls are placed from within the United States to non-U.S. persons abroad. Non-U.S. persons outside the United States may be freely surveilled by the NSA without even a FISA warrant; therefore, when an unidentified U.S. person places a call to an alien outside the United States who is being surveilled by the NSA lawfully without a warrant, the NSA then automatically and inadvertently surveils that U.S. person. In such a situation, serious questions arise as to the extent to which information

\begin{itemize}
\item \textsuperscript{8} FISA’s provisions require the government to obtain a FISA warrant when seeking to surveil a “United States person.” A U.S. person is defined as a U.S. citizen, a permanent resident, a corporation incorporated in the United States, or an unincorporated association consisting of mostly U.S. citizens or permanent residents. FISA, 50 U.S.C. § 1801(i) (2000).
\item \textsuperscript{10} The Fourth Amendment does not place any restraints on the power of the government to surveil non-U.S. persons outside the United States. United States v. Verdugo-Urquidez, 494 U.S. 259, 274–75 (1990) (holding that aliens outside U.S. territory are not entitled to any protection under the Fourth Amendment).
\item \textsuperscript{11} See FISA, 50 U.S.C. § 1801(i) (defining “United States person” as “a citizen of the United States, 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, but does not include a corporation or an association which is a foreign power”).
\item \textsuperscript{12} FISA allows non-U.S. persons to be surveilled in the United States without a FISA warrant based solely upon certification by the Attorney General. See FISA, 50 U.S.C.A. § 1802(a) (West 2001 & Supp. 2005). If, however, there is a substantial likelihood that a U.S. person’s communication will be surveilled in the course of these efforts, the government must seek approval from the Foreign Intelligence Surveillance Court. See FISA, 50 U.S.C. § 1802(b); see also FISA, 50 U.S.C.A. § 1804 (detailing the requirements for FISA warrant applications).
\end{itemize}
gained from such efforts may be used subsequently against that U.S. person.

The NSA’s attempt to answer these questions can be found in the agency’s minimization procedures, which are detailed in United States Signals Intelligence Directive 18 (“USSID 18”). Under most circumstances, the directive requires the NSA to destroy information gained inadvertently from unsuspecting U.S. persons without a warrant; however, section 7.2(c)(4) allows the agency to disseminate such “inadvertently acquired” information to U.S. law enforcement if it appears to implicate the U.S. person in criminal conduct.

This Article discusses this loophole in light of recent advancements in encrypted Voice over Internet Protocol (“VoIP”) technology. It concludes that the minimization procedures set forth in USSID 18 are constitutionally deficient because they fail to take into account the growing expectation of privacy that has resulted from advancements in encryption technology. The directive should be redrafted to mandate greater consideration of an individual’s reasonable expectation of privacy when determining how information collected without a warrant may be disseminated and used by the agency.

This Article is comprised of four parts. Part I provides an explanation of the NSA and its signals intelligence activities. Part II discusses the legal framework for the electronic surveillance operations of the NSA and explains the loophole that allows the agency to seize and analyze international communications made by U.S. citizens without a warrant. Part III examines encrypted Internet telephony, cryptanalysis, and the territorial limits of constitutional rights. Part IV discusses the constitutionality of section 7.2(c)(4) of USSID 18 as applied to encrypted Internet telephony. The Article then concludes by proposing that communication via encrypted Internet telephony offers the user such a reasonable expectation of privacy that the Fourth Amendment should extend to prevent dissemination of information pertaining to U.S. persons gained from the warrantless

---

14 Id. § 3.1.
15 Id. § 7.2(c)(4).
16 See infra notes 21–50 and accompanying text.
17 See infra notes 51–144 and accompanying text.
18 See infra notes 145–191 and accompanying text.
19 See infra notes 192–232 and accompanying text.
capture of such communications—except in very limited situations where truly exigent circumstances exist.\(^{20}\)

I. Background: Signals Intelligence and the NSA

Signals intelligence, or SIGINT, refers to intelligence acquired through the capture of electronic signals.\(^{21}\) The term encompasses three categories of intelligence information: communications intelligence (“COMINT”); electronics intelligence (“ELINT”); and foreign instrumentation signals intelligence (“FISINT”).\(^{22}\) The NSA is the agency responsible for the signals intelligence operations of the United States.\(^{23}\) In addition to the initial gathering of signals, SIGINT operations often involve subsequent cryptanalysis\(^{24}\) which is performed by the Central Security Service (the “CSS”),\(^{25}\) a component sub-agency of the NSA that brings together the cryptographic and cryptanalytic capabilities of the Army, Navy, Marines, and Air Force.\(^{26}\)

Although the scope of the NSA’s SIGINT operations has always been the subject of wild speculation, the true number of communications intercepted by the agency has remained a closely guarded secret. Speculation about the number of communications intercepted by the NSA began to grow when rumors of a global signals intelligence network involving multilateral cooperation between several nations be-

\(^{20}\) See infra notes 225–238 and accompanying text.


\(^{22}\) See id. “Communications intelligence” or “COMINT” is a subset of the broader discipline of signals intelligence that deals specifically with the capture of encrypted communications for intelligence purposes. Although “communications intelligence” is probably a more apt description of the specific type of operations at issue in this Article, the term is often used interchangeably with “signals intelligence” in common parlance, so I have chosen to use the latter throughout this Article to be certain to cover all relevant NSA operations.


\(^{24}\) Cryptanalysis is defined as “[t]he conversion of encrypted messages into plain text without having the initial knowledge of the key used in encryption.” Nat’l Sec. Agency/Cent. Sec. Serv., Frequently Asked Questions About NSA, http://www.nsa.gov/about/about00018.cfm#18 (last visited Mar. 23, 2006).

\(^{25}\) Although the combined National Security Agency and Central Security Service are often referred to as the NSA/CSS, the two entities will be discussed collectively as the “NSA” throughout most of this Article for the purpose of simplicity.

\(^{26}\) Nat’l Sec. Agency/Cent. Sec. Serv., supra note 24.
gan to surface in 1988. In that year, Margaret Newsham, a former contract employee working at the NSA field station in Menwith Hill, Yorkshire, England, complained to the U.S. House Permanent Select Committee on Intelligence about alleged corruption and impropriety surrounding the use of the NSA’s signals intelligence resources. She claimed to have witnessed employees of the agency intercepting a telephone call placed by then-U.S. Senator Strom Thurmond. Her allegations also included details of a global surveillance system known as ECHELON. This fueled public interest and a large number of newspaper articles, but the agency remained silent about the system, and media coverage fizzled shortly thereafter.

In recent years, several high-profile investigative reports have rekindled public interest in the ECHELON network. For example, in 2000, the CBS program 60 Minutes aired a feature on the ECHELON system. The program included an interview with Mike Frost, a former twenty-year employee of Canada’s principal signals intelligence agency, the Communications Security Establishment (the “CSE”). During the interview, Frost made revelations about the specific capabilities of the ECHELON system, stating at one point that the system captures “everything . . . from data transfers to cell phones to portable phones to baby monitors to ATMs.” Frost had been one of the first insiders to divulge specifics about the breadth of ECHELON’s surveillance capabilities, and his account helped to spark renewed public interest in the system.

---

27 The NSA’s Menwith Hill Station in Yorkshire, England, is rumored to be the largest signals intelligence facility in the world. 60 Minutes: ECHELON; Worldwide Conversations Being Received by the ECHELON System May Fall into the Wrong Hands and Innocent People May Be Tagged as Spies (CBS television broadcast Feb. 27, 2000) [henceforth 60 Minutes].


29 See id.

30 See generally Mike Frost, Spyworld: Inside the Canadian & American Intelligence Establishments (1994) (giving Frost’s first account of some of the operations of Canada’s Communications Security Establishment (the “CSE”) and the NSA).

31 Id.

32 60 Minutes, supra note 27.

33 Id.

34 Id.

35 See generally Frost, supra note 31 (offering an account of the operations between the CSE and the NSA). Although much of the controversy surrounding ECHELON is relatively recent, multilateral SIGINT collaboration between these nations is nothing new. Their cooperation began with the BRUSA COMINT Alliance between the United States and the British Commonwealth, which was created at the end of World War II. See Lawrence D. Sloan, Note, ECHELON and the Legal Restraints on Signals Intelligence: A Need for Reevaluation, 50 Duke L.J.
News reports concerning the ECHELON system raised concerns in Europe, and on July 5, 2000, the European Parliament established a temporary committee to investigate.\textsuperscript{36} Approximately one year later, this committee issued its “Report on the Existence of a Global System for the Interception of Private and Commercial Communications.”\textsuperscript{37} The report detailed the existence of ECHELON, its legality under European and international law, and its implications for the privacy rights of European citizens.\textsuperscript{38} Subsequently, the European Union began seeking ways to counter the effects of ECHELON through enhanced encryption protocols.\textsuperscript{39} In 2004, the European Union created the SECOQC project.\textsuperscript{40} Under the project, the European Union will spend $11 million on research and development for a new quantum encryption system that could be used to thwart the signals intelligence capabilities of ECHELON.\textsuperscript{41}

The ECHELON system is rumored to capture as many as three billion communications each day.\textsuperscript{42} The system’s reach spans the globe due to the strategic locations of its five member nations, which

\begin{itemize}
\item \textsuperscript{37} Id.
\item \textsuperscript{38} Id.
\item \textsuperscript{40} SECOQC Stands for Secure Communication Based on Quantum Cryptography. SECOQC Home Page, http://www.secoqc.net (last visited Mar. 23, 2006).
\item \textsuperscript{41} See Chesterman, supra note 35, at 21 (discussing the European Union’s efforts to secure communications through quantum cryptography); see also Willan, supra note 39, (discussing the European Union’s plans to develop a secure communication system that would be immune from the interception capabilities of ECHELON). This move by the European Union seems to be fueling competition between technology firms to develop new and better forms of data encryption. See R. Colin Johnson, Quantum Encryption Enters Product Phase, Electronic Engineering Times, May 2, 2005, at 44 (discussing the Infosecurity Europe 2005 trade show in London, where a new turnkey quantum encryption system and other encryption innovations were unveiled).
\item \textsuperscript{42} Vernon Loeb, Critics Questioning NSA Reading Habits; Politicians Ask if Agency Sweeps in Private Data, Wash. Post, Nov. 13, 1999, at A3.
\end{itemize}
include the United States, the United Kingdom, Canada, Australia, and New Zealand.\textsuperscript{43} Together, these nations comprise the UKUSA community, which has its roots in the BRUSA COMINT alliance established between the United States and the British Commonwealth during World War II.\textsuperscript{44} Through satellite and other means, ECHELON is believed to be capable of capturing most electronic signals broadcast anywhere in the world.\textsuperscript{45}

The NSA has refused to comment on ECHELON, even invoking attorney-client privilege to avoid compliance with document requests made by the U.S. House Permanent Select Committee on Intelligence.\textsuperscript{46} Such actions have fueled speculation by conspiracy theorists, as well as concern on the part of civil libertarians.\textsuperscript{47} Although most estimates about the exact capabilities of ECHELON are likely exaggerated by these groups, the amount of data collected by the joint efforts of the UKUSA community is probably much more substantial than imagined before the existence of ECHELON came to light.\textsuperscript{48} Consequently, due to the large volume of international communications potentially being captured by ECHELON, there is a substantial likelihood

\textsuperscript{43}There are five agencies that participate in collective signals operations through the ECHELON network. They are the United States’ NSA, the United Kingdom’s GCHQ, Canada’s CSE, Australia’s Defence Signals Directorate (“DSD”), and New Zealand’s Government Communications Security Bureau (“GCSB”). See Chesterman, \textit{supra} note 35, at 22; see also Sloan, \textit{supra} note 35, at 1471 (discussing the global reach of ECHELON that results from multinational, cooperative intelligence gathering).

\textsuperscript{44}E.U. Report, \textit{supra} note 36, at 60–61; see also Chesterman, \textit{supra} note 35, at 22 (providing a detailed history of UKUSA signals intelligence cooperation).

\textsuperscript{45}See E.U. Report, \textit{supra} note 36, at 34.

\textsuperscript{46}On August 31, 1999, U.S. Representative Bob Barr (R-Ga.) was interviewed by Fox News host Bill O’Reilly and was asked about the House Intelligence Committee’s attempts to discover more information about the ECHELON network. He stated that “when the House Intelligence Committee did ask the NSA for the justification and an explanation of this program, not only did they refuse to give it to them, but—get this—their rationale was ‘We can’t give it to you because that’s attorney-client privilege.’” \textit{The O’Reilly Factor: Unresolved Problem: Project ECHelon} (Fox News Channel television broadcast Aug. 31, 1999); see also John C. K. Daly, \textit{ECHelon—The Ultimate Spy Network?}, UNITED PRESS INT’L, Mar. 1, 2004 (describing the U.S. government’s “terse ‘no comment’ attitude to all inquiries regarding Echelon”).

\textsuperscript{47}Many civil liberties groups have expressed concern over the NSA’s reluctance to reveal details about the operation of the ECHELON system. After the NSA’s refusal to disclose documents, the American Civil Liberties Union, the Electronic Privacy Information Center, and the Omega Foundation created EchelonWatch.org, a website dedicated to tracking the system. See Robert MacMillan, \textit{ACLU Plans to Observe Echelon Global Spy Net Online}, Newsbytes, Nov. 16, 1999.

\textsuperscript{48}See E.U. Report, \textit{supra} note 36, at 34 (“If UKUSA States operate listening stations in the relevant regions of the earth, in principle they can intercept all telephone, fax, and data traffic transmitted via such satellites.”).
that a significant number of international phone calls made to and from American citizens were being collected by the NSA even before President Bush issued his secret executive order.\footnote{Even prior to the controversial order, it was possible for the NSA to keep and disseminate information collected about U.S. citizens although no warrant authorized the initial surveillance. \textit{See} USSID 18, \textit{supra} note 13, § 3.1.} The next Part details the legal structure that regulates the NSA’s signals intelligence efforts and describes the situations where U.S. citizens might have their conversations monitored by the agency without a warrant.\footnote{See \textit{infra} notes 51–144 and accompanying text.}

II. The Legal Framework Governing NSA SIGINT Operations

The NSA’s electronic surveillance activities are governed primarily by four authorities: the U.S. Constitution,\footnote{See \textit{U.S. Const. amend. IV.}} FISA,\footnote{See \textit{FISA}, 18 U.S.C.A. §§ 2511, 2518, 2519, 50 U.S.C.A. §§ 1801–1811, 1821–1829, 1841–1846, 1861–1862, 1871 (West 2001 & Supp. 2005).} Executive Order No. 12,333,\footnote{See \textit{Exec. Order No. 12,333, 3 C.F.R. 200 (1982), reprinted in 50 U.S.C. § 401 note (2000).}} and USSID 18.\footnote{See \textit{USSID 18, supra} note 13.} The Fourth Amendment and FISA provide a high degree of protection for U.S. persons inside the United States and a slightly lower degree of protection for U.S. persons located outside U.S. borders.\footnote{Courts have held that the government may use evidence collected by foreign governments against U.S. persons at trial in the United States even though such evidence was collected in a manner that would have violated their constitutional rights if conducted by U.S. agents. \textit{See} Stefan Epstein, \textit{Annotation, Application of Fourth Amendment Exclusionary Rule to Evidence Obtained Through Search Conducted by Official of Foreign Government, 33 A.L.R. Fed. 342, § 3(a) (1977)} (explaining the general rule that the exclusionary rule does not apply to searches conducted by foreign governments). This is true even if U.S. agents are involved with the foreign government’s efforts, provided that their participation is not substantial. \textit{See id.; see also Gov’t of Canal Zone v. Sierra, 594 F.2d 60, 72 (1979)} (“Fourth Amendment rights are generally inapplicable to an action by a foreign sovereign in its own territory in enforcing its own laws, even though American officials are present and cooperate in some degree.”). Also, traffic stops and questioning conducted by U.S. border officials on U.S. citizens entering and leaving the country have been upheld as constitutional despite the absence of probable cause or reasonable suspicion. United States v. Martinez-Fuerte, 428 U.S. 543, 566 (1976) (holding that the use of fixed border checkpoints and the questioning of travelers at U.S. borders do not require warrants or probable cause). The Supreme Court has also held that the government may hand over an American soldier for trial by a foreign government although U.S. constitutional guarantees will not be provided. Wilson v. Girard, 354 U.S. 524, 530 (1957).}
surveillance by U.S. intelligence agencies. Therefore, international telephone calls from U.S. citizens inside the United States to foreign acquaintances abroad could be captured by the NSA without a warrant if those foreign acquaintances are under NSA surveillance. In such a situation, the only protections currently afforded to U.S. citizens are found in the minimization procedures mandated by FISA and Executive Order No. 12,333. The specific minimization procedures applicable to NSA operations are detailed in USSID 18. Each of the four legal authorities—and the protections they provide—are discussed individually below.

A. The Fourth Amendment

The Fourth Amendment to the U.S. Constitution lays the foundation for all legal restrictions on the NSA’s electronic surveillance and signals intelligence operations. It ensures the right of U.S. persons to be free from unreasonable searches and seizures, and mandates that no warrants be issued absent a showing of probable cause. Prior to 1967, electronic surveillance was not considered to be a “search” for purposes of the Fourth Amendment. However, in 1967, the Supreme Court extended the definition to include electronic surveillance, thereby requiring all government agencies to obtain a warrant prior to conducting such surveillance on U.S. persons.

---


59 USSID 18, supra note 13.

60 See U.S. Const. amend. IV.

61 Id. (“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 . . . .”).


The rights protected by the Fourth Amendment are subject to some important limitations. For example, since World War II, U.S. presidents have asserted that the executive branch has the power to order warrantless electronic surveillance when national security is at stake.\(^64\) This exception has become known as the national security exception to the Fourth Amendment.\(^65\) Although the exception is not specifically enumerated in the Constitution, caselaw has recognized a limited set of circumstances under which the President’s power to control foreign affairs may allow warrantless searches to be ordered to effectuate that purpose.\(^66\) Courts have, however, allowed the exception to be invoked only in a limited set of situations, all of which have involved some form of foreign security effort.\(^67\) Moreover, the Supreme Court has specifically refused to recognize the national security exception in cases involving domestic surveillance operations targeting American citizens within U.S. borders.\(^68\) For instance, in 1972, in United States v. U.S. District Court (Keith), the Supreme Court held that the President’s power to protect national security did not eliminate the need for the Central Intelligence Agency to obtain a warrant before conducting electronic surveillance of suspected terrorists within the territorial boundaries of the United States.\(^69\) This holding proved


\(^{65}\) See id.

\(^{66}\) See id.

\(^{67}\) See 68 Am. Jur. 2d Searches and Seizures § 161 (2005); see also United States v. Totten, 92 U.S. 105, 106 (1875) (recognizing the President’s power to conduct foreign affairs includes the power to authorize foreign intelligence operations and the use of clandestine agents); United States v. Sinclair, 321 F. Supp. 1074, 1079 (E.D. Mich. 1971) (“Presidential power of surveillance is specifically limited to ‘exceptional cases’—cases of a non-criminal nature or which concern the country’s national security.”).

\(^{68}\) See 68 Am. Jur. 2d Searches and Seizures § 161 (2005) (“Generally, there is no clearly announced ‘national security’ exception to the requirement of a search warrant. To the extent there is such an exception, it may only be invoked by the special authorization of the President or the Attorney General of the United States. The distinguishing element between domestic security cases, in which no exception to the warrant requirement exists, and cases involving foreign security, in which an exception may exist, is whether the activities of the subject at which the search is directed affect the foreign relations of the United States.”) (footnotes omitted). Compare United States v. Ehrlichman, 376 F. Supp. 29, 35 (D.D.C. 1974) (refusing to recognize a broad interpretation of the national security exception), with United States v. Butenko, 494 F.2d 593, 605–06 (3d Cir. 1974) (holding that a warrant was not required in a case involving surveillance conducted for foreign intelligence purposes, but reasoning that if members of a domestic political organization were the subject of such surveillance unrelated to foreign affairs, such surveillance would “undoubtedly be illegal”).

problematic for U.S. intelligence agencies, which feared that seeking a warrant through traditional avenues would require divulging secret information about agency methods and ongoing operations. The Keith Court had, however, specifically refused to address the issue of whether the agency was required to obtain a traditional warrant in matters involving foreign powers or agents, which left room for Congress to step in and create an alternative means of satisfying the warrant requirement while also protecting classified information.

Accordingly, with FISA’s passage in 1978, Congress provided U.S. agencies with an alternative means of obtaining warrants for foreign intelligence surveillance operations targeting U.S. persons. Another purpose of the Act was to prevent abuses by the executive branch, which had engaged in domestic surveillance of civil rights and antiwar activists during the Vietnam era. FISA established strict procedural rules for conducting electronic surveillance for foreign intelligence and counterintelligence purposes within the United States.

It is important to note that FISA does not apply to foreign surveillance operations that target non-U.S. persons located abroad. FISA merely provides a procedural framework for satisfying the requirements of the Fourth Amendment, and the Fourth Amendment does not extend protection to non-U.S. persons outside the territorial limits of the United States.

70 See id. at 319 (quoting a brief for the United States as stating that being required to obtain search warrants in these cases would require disclosures to magistrates that “would create serious potential dangers to the national security and to the lives of informants and agents”).

71 In Keith, the Supreme Court held that the government was required to obtain a warrant to conduct domestic surveillance related to national security, but it refused to address the issue of a warrant requirement for foreign cases. Specifically, the Court stated, “this case involves only the domestic aspects of national security. We have not addressed, and express no opinion as to, the issues which may be involved with respect to activities of foreign powers or their agents.” Id. at 321–22.

72 See id.; cf. Zweibon v. Mitchell, 516 F.2d 594, 654–55 (D.C. Cir. 1975) (refusing to extend the national security exception to allow a warrantless search of people who were not agents of a foreign power).


74 See id.; Risen & Lichtblau, supra note 2, at A1.


Therefore, there are virtually no constitutional limits on the ability of the NSA—or any other U.S. agency—to conduct electronic surveillance or even property seizures on non-U.S. persons abroad. Consequently, FISA’s warrant requirement does not apply to situations where a non-U.S. person is the target of NSA surveillance outside the United States, even if U.S. persons may be inadvertently surveilled as a result.

B. The Foreign Intelligence Surveillance Act of 1978

FISA applies to all instances of electronic surveillance performed by government agents within the United States for foreign intelligence purposes. Its procedural framework is distinct from that governing the conduct of electronic surveillance for general law enforcement purposes, which is instead governed primarily by two other congressional acts: Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (“Title III”) and the Electronic Communications Privacy Act of 1986 (the “ECPA”). Title III was passed in 1968 in order to regulate surveillance of oral communications. Additionally, in 1986, Congress passed the ECPA, which amended Title III and extended its scope to cover the new forms of electronic communication presented by increased computer usage. These two statutes provide guidance to U.S. law enforcement and intelligence agencies seeking to conduct domestic surveillance for law enforcement purposes. Although some assistance is allowed, the NSA is generally not permit-

---

78 See id. (holding that the Fourth Amendment does not apply to physical searches or seizures against non-U.S. persons located outside the United States); see also United States v. Truong Dinh Hung, 629 F.2d 908, 915–16 (4th Cir. 1980) (upholding the warrantless surveillance of a non-U.S. citizen who was an agent of the Vietnamese government).
79 See Verdugo-Urquidez, 494 U.S. at 274–75; Truong Dinh Hung, 629 F.2d at 915–16.
ted to conduct signals intelligence operations within the United States for the purpose of general domestic law enforcement.\textsuperscript{86} NSA operations are typically confined to foreign intelligence, counterintelligence, or counterterrorism purposes.\textsuperscript{87} As a result, the NSA’s domestic ECHELON operations are primarily governed by FISA.

Although the NSA is not generally permitted to conduct domestic surveillance for law enforcement purposes, information about U.S. citizens obtained under a FISA warrant may be used in criminal proceedings against them.\textsuperscript{88} The information sought to be used need not be evidence of a crime related to espionage. The only limitation is that the collection of foreign intelligence information must have been a “significant” purpose of the FISA surveillance.\textsuperscript{89} Prior to the passage of the USA PATRIOT Act in 2001,\textsuperscript{90} the collection of foreign intelligence

\textsuperscript{86} USSID 18, \textit{supra} note 13, § 1.4 (“[T]he focus of all foreign intelligence operations is on foreign entities and persons.”). However, NSA assistance to law enforcement is permitted in a limited number of circumstances. \textit{See} 10 U.S.C. § 371 (2000) (permitting the Secretary of Defense to provide law enforcement agencies with information collected by Department of Defense components if that information is relevant to narcotics trafficking).

\textsuperscript{87} USSID 18, \textit{supra} note 13, § 3.1 (“The policy of the [U.S. SIGINT System] is to target or collect only foreign communications. The USSS will not intentionally collect communications to, from or about U.S. persons or persons or entities in the U.S. except as set forth in this [U.S. Signals Intelligence Directive].”).


\textsuperscript{90} Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Pub. L. No. 106-56, 115 Stat. 272 (codified as
information needed to be the “primary purpose” of FISA surveillance. Now, it need only be a “significant purpose” of the surveillance in order for a FISA warrant to be issued. This change drastically increased the ease with which government agents can obtain domestic surveillance warrants under FISA.

FISA was intended to govern every instance of electronic surveillance conducted by U.S. agents within the territorial boundaries of the United States for foreign intelligence or counterintelligence purposes. Section 201(b) of the Act states that FISA “shall be the exclusive means by which electronic surveillance . . . and the interception of domestic wire and oral communications may be conducted.” The Act set forth procedures through which the government may seek authorization for such surveillance without being required to follow the traditional warrant procedures mandated by the Fourth Amendment. Congress believed this step was necessary to protect sensitive national security information that might otherwise be revealed under the traditional warrant issuance framework.


91 FISA, 50 U.S.C. § 1804(a)(7) (2000 & Supp. III 2003) (stating that applications for FISA warrants must include a certification by an executive branch official verifying that “the certifying official deems the information sought to be foreign intelligence information” and that “a significant purpose of the surveillance is to obtain foreign intelligence information”).

92 FISA, 18 U.S.C. § 2511(2)(f) (amending the Omnibus Crime Control and Safe Streets Act of 1968 to provide that FISA “shall be the exclusive means by which electronic surveillance . . . and the interception of domestic wire, oral, and electronic communications may be conducted”). In 1994, FISA was amended to allow the FISC to issue warrants for physical searches as well as electronic surveillance. See Intelligence Authorization Act for Fiscal Year 1995, Pub. L. No. 103-359, § 807(a)(3), 108 Stat. 3423, 3443–44 (1994) (codified at 50 U.S.C. § 1822 (2000)) (amending FISA to add a new Title III concerning physical searches, giving the President the power to “authorize physical searches without a court order . . . to acquire foreign intelligence information for periods of up to one year”).


94 FISA, 50 U.S.C.A. § 1802 (West 2001 & Supp. 2005) (providing that “the President, through the Attorney General, may authorize electronic surveillance without a court order . . . to acquire foreign intelligence information for periods of up to one year” if certain conditions are fulfilled and certain procedures are followed).

95 See S. Rep. No. 95-604, at 15 (1977). For example, when a U.S. intelligence agency decides to conduct electronic surveillance for foreign intelligence or counterintelligence purposes, that decision is usually based on classified information. The traditional process for obtaining a warrant for such searches would almost invariably involve the disclosure of secret information, which would divulge current intelligence collection efforts and methods. An alternative to the traditional warrant procedures was necessary to preserve national security. FISA provided that alternative.
As part of this procedural framework, FISA established a special court known as the Foreign Intelligence Surveillance Court (the “FISC”). This court hears most government requests to conduct “electronic surveillance” within the United States for foreign intelligence purposes. The Act also mandated the adoption of minimization procedures to limit the effects of FISA-authorized surveillance on U.S. persons. FISA does not, however, extend protection to non-U.S. persons outside the United States. Collecting signals information outside U.S. borders is not considered “electronic surveillance” under the Act’s definition, even if a U.S. person is specifically targeted.

Although NSA collection efforts under FISA may target only those suspected of being agents of a foreign government or terrorist organization, the Act allows the agency to use unrelated information that is inadvertently acquired about U.S. citizens who are not the proper tar-


98 See 50 U.S.C. §§ 1801(h), 1802(a)(1)(C), 1804(a)(5).

99 See supra note 9 and accompanying text; see also United States v. Bin Laden, 126 F. Supp. 2d 264, 287 n.26 (S.D.N.Y. 2000) (discussing how searches conducted in Kenya are not governed by FISA).

100 See FISA, 50 U.S.C. § 1801(f). Section 1801(f) of FISA defines four types of conduct that are considered “electronic surveillance” under FISA. Signals collection operations that target U.S. persons outside the United States do not fit within any of these four definitions. The first three definitions require the targeted individual to be located inside of the United States to be considered “electronic surveillance.” The fourth definition applies only to the use of surveillance devices within the United States. Therefore, the NSA’s signals monitoring stations in the United Kingdom, Canada, Australia, and New Zealand are not regulated by FISA. U.S. personnel located at these foreign stations presumably may monitor U.S. persons who are outside the United States, and that conduct technically would not be considered electronic surveillance under FISA’s definitions. This highlights the fact that FISA was meant to govern only domestic surveillance taking place within U.S. borders. Although such efforts would not fall under FISA’s definition of “electronic surveillance,” USSID 18’s minimization procedures still would apply and offer some protection to the rights of U.S. persons abroad. See generally USSID 18, supra note 13.
gets of the surveillance.\footnote{Although FISA requires the use of minimization procedures to limit the impact of authorized surveillance on U.S. persons who are not named as targets, the Act specifically allows evidence of a crime to be disseminated and used by law enforcement. FISA, 50 U.S.C. § 1801(h)(3). Evidence collected pursuant to a valid FISA warrant may be used in criminal proceedings against persons who were not named in the warrant as targets of the authorized surveillance. See id. § 1806(g) (stating that a motion to exclude evidence collected pursuant to a FISA warrant shall be denied if the surveillance was lawfully authorized and conducted); see also United States v. Isa, 923 F.2d 1300, 1304 (8th Cir. 1991) (“There is no requirement that the ‘crime’ be related to foreign intelligence.”); United States v. Badia, 827 F.2d 1458, 1464 (11th Cir. 1987) (holding that evidence collected pursuant to a FISA warrant issued against one individual is admissible as evidence against an acquaintance with whom the individual had spoken during the period of the surveillance).} If the NSA wishes to use such information obtained during FISA-authorized surveillance, it must comply with its own FISA-related minimization procedures, which are located in Annex A to USSID 18.\footnote{USSID 18, supra note 13, at Annex A, app. 1, § 1 (“These procedures apply to the acquisition, retention, use, and dissemination of non-publicly available information concerning unconsenting United States persons that is collected in the course of electronic surveillance as ordered by the United States Foreign Intelligence Surveillance Court under Section 102(b) or authorized by Attorney General Certification under Section 102(a) of [FISA].”).} The procedures in Annex A apply only to information acquired during domestic FISA surveillance conducted pursuant to a FISA warrant.\footnote{FISA allows the use of information about any U.S. person that is collected pursuant to a FISA warrant provided that such use is conducted in accordance with applicable minimization procedures. Id. § 1806(a). FISA applies only to surveillance conducted inside the United States. Executive Order No. 12,333 mandated that additional minimization procedures be implemented in all U.S. intelligence agencies. Exec. Order No. 12,333, § 2.3, 3 C.F.R. 200, 211 (1982), reprinted in 50 U.S.C. § 401 note (2000). These minimization procedures apply to all surveillance regardless of its location. See id. Directive No. 5240.1 is the Department of Defense’s implementation of the Order’s requirements. U.S. Dep’t of Defense, Directive No. 5240.1 (Apr. 1988) [hereinafter DoD Directive No. 5240.1], available at http://www.dtic.mil/whs/directives/corres/pdf/d52401_042588/d52401p.pdf. Directive 5240.1 applies to all intelligence activities of Department of Defense components, including the NSA. See id. Regulation No. 5240.1-R is a detailed regulation that implements Directive No. 5240.1, and this document is tied to a previous version of [FISA].”)}

Non-FISA surveillance against non-U.S. persons abroad may be conducted lawfully without a warrant; however, these operations must still be conducted in a manner that minimizes the impact on the rights of unintentionally monitored U.S. persons.\footnote{See FISA, 50 U.S.C. § 1801(h) (2000 & Supp. III 2003).} In order to use inadvertently acquired information pertaining to U.S. persons gained through warrantless foreign surveillance, the agency must comply with the minimization procedures mandated by Executive Order No. 12,333 and Department of Defense Directive 5240.1.\footnote{See FISA, 50 U.S.C. § 1801(h) (2000 & Supp. III 2003).}
C. Executive Order No. 12,333

The lawfully warrantless foreign surveillance activities of the NSA that are not governed by FISA are governed by Executive Order No. 12,333. President Ronald Reagan issued the order in 1981 in an attempt to provide a clear presidential statement about the duties and responsibilities of the agencies involved in the national intelligence effort and to mandate the adoption of internal administrative minimization procedures applicable to all surveillance efforts conducted by members of the U.S. Intelligence Community. Similar executive orders issued by Presidents Ford and Carter during their administrations preceded Executive Order No. 12,333. Unlike its predecessors, however, Executive Order No. 12,333 has remained in force and virtually unchanged since its issuance in 1981. It has represented the principal executive-branch statement regarding the appropriate scope of U.S. intelligence agency operations for the last twenty-five years.

In addition to containing broad pronouncements about the goals and duties of the different components of the U.S. intelligence apparatus, Executive Order No. 12,333 also places specific limitations on the proper means of conducting intelligence collection. For example, it authorizes the NSA, as a member of the U.S. Intelligence Community, to collect and disseminate information about U.S. citizens for foreign intelligence and counterintelligence purposes, but it limits such collection efforts to those conducted in accordance with the procedures set forth by the Director of the NSA and the Attorney General. Further, it gives the Attorney General the power to approve the use of electronic surveillance upon his or her own determination that there is probable cause to believe that the surveillance is to be used against a foreign...
power or agent.112 The order also requires, however, the Attorney General to comply with the minimization requirements imposed by FISA.113

With respect to ECHELON, the restrictions imposed by Executive Order No. 12,333 and FISA apply only to situations where the NSA seeks to conduct surveillance within the United States or against U.S. persons abroad.114 Virtually no restrictions are placed on the ability of the agency to conduct such surveillance on non-U.S. persons located outside the territorial limits of the United States.115 Because the NSA is allowed to conduct virtually unfettered surveillance of foreign persons outside the United States, American citizens may be inadvertently surveilled by the NSA without a warrant whenever they communicate with foreign persons located in other countries.116 Even assuming that the NSA does not routinely engage in the interception of domestic U.S. signals, the capture of so many foreign communications still results in the collection, without a warrant, of a significant number of phone calls made to and from U.S. persons each year.117 Presumably, such situations occurred even prior to President Bush’s issuance of the secret executive order allowing warrantless domestic surveillance in apparent violation of FISA.118

115 FISA, 50 U.S.C. § 1801(f); Exec. Order No. 12,333, § 2.4, 3 C.F.R. 200, 212 (1982), reprinted in 50 U.S.C. § 401 note (2000); see also Verdugo-Urquidez, 494 U.S. at 274–75 (reasoning that the Fourth Amendment did not apply to a Mexican citizen when the place searched was in Mexico).
116 Justice Brandeis’ dissent in Olmstead v. United States provides an illustration of this point. See 277 U.S. at 471–85 (Brandeis, J., dissenting). He explained that

The evil incident to invasion of the privacy of the telephone is far greater than that involved in tampering with the mails. Whenever a telephone line is tapped, the privacy of the persons at both ends of the line is invaded, and all conversations between them upon any subject, and although proper, confidential, and privileged, may be overheard. Moreover, the tapping of one man’s telephone line involves the tapping of the telephone of every other person whom he may call, or who may call him.

Id. at 475–76.
117 See Loeb, supra note 42, at A3.
118 See id.
Although the likelihood for the warrantless seizure of international communications involving U.S. citizens seems quite high, the agency has adopted internal safeguards to limit the adverse effects of ECHELON’s massive signals intelligence operations with respect to the rights of U.S. citizens. These internal safeguards, mandated by both Executive Order No. 12,333 and Department of Defense Directive 5240.1, are embodied in USSID 18.

D. United States Signals Intelligence Directive 18 (USSID 18)

USSID 18 sets forth the primary operating guidelines that govern the signals intelligence operations of the NSA. FISA and Executive Order No. 12,333 require these “minimization procedures” in order to reduce the “acquisition and retention, and prohibit the dissemination, of nonpublic information concerning unconsenting United States persons.” Accordingly, the NSA’s primary objective in detailing these procedures is to minimize the impact on U.S. persons caused by the otherwise legitimate warrantless electronic surveillance routinely conducted by the NSA on non-U.S. persons abroad. Fundamentally, USSID 18 is an attempt to strike a balance between the often competing interests of Fourth Amendment privacy guarantees and U.S. national security.

It is the stated policy of the NSA “to target or collect only foreign communications.” USSID 18 makes clear that the NSA “will not intentionally collect communications to, from or about U.S. persons or persons or entities in the United States,” except as allowed under its provisions. Although the NSA generally may not intentionally collect the communications of U.S. persons without a FISA warrant, USSID 18 specifically states that the agency may collect such communications unintentionally. More specifically, section 3.1 of USSID 18 states that if the NSA “inadvertently” collects communications made to or from U.S. persons who were not the lawful target of the surveillance efforts, the

---

120 See generally DoD Directive No. 5240.1, supra note 105.
121 See generally USSID 18, supra note 13.
122 Id.
124 See USSID 18, supra note 13, § 1.2.
125 See id.
126 Id. § 3.1.
127 Id.
128 See id.
agency may still retain, analyze, and disseminate such information under certain circumstances.\textsuperscript{129}

Most of these specific situations are unknown because they seem to be enumerated in sections 4.4 to 4.7 of USSID 18, which have been redacted from the declassified version of the directive.\textsuperscript{130} Some indications may be gleaned, however, from other declassified provisions.\textsuperscript{131} For instance, USSID 18’s definition of “foreign communication” provides some indication of the types of communications allowed to be retained.\textsuperscript{132} Section 9.8 defines a foreign communication as “a communication that has at least one communicant outside the United States . . . .”\textsuperscript{133} Although surveillance efforts directed at premises in the United States are not considered foreign communications under the definition, efforts aimed at foreign residences, which inadvertently result in the collection of calls to and from U.S. persons, clearly remain part of the definition.\textsuperscript{134} The fact that these communications are considered “foreign communications” is significant because it is the stated policy of the NSA to “target or collect only foreign communications.”\textsuperscript{135} Because ECHELON and other NSA signals intelligence efforts are estimated to collect most foreign communications transmitted worldwide, the “inadvertent” surveillance of U.S. persons placing international telephone calls can be assumed to be quite frequent.\textsuperscript{136}

In order to mitigate the effects of this unavoidable consequence of the NSA’s foreign intelligence efforts, USSID 18 section 7.1 provides that “foreign intelligence information concerning U.S. persons must be disseminated in a manner which does not identify the U.S. person.”\textsuperscript{137} This is typically accomplished by redacting the U.S. person’s name or by similar means.\textsuperscript{138} USSID 18 does, however, allow dis-

\begin{itemize}
\item \textsuperscript{129} USSID 18, supra note 13, § 3.1.
\item \textsuperscript{130} See id. §§ 4.4–4.7.
\item \textsuperscript{131} See id. § 9.8.
\item \textsuperscript{132} See id.
\item \textsuperscript{133} Id. The definition also includes communications that are “entirely among foreign powers or between a foreign power and officials of a foreign power . . . .” Id.
\item \textsuperscript{134} See USSID 18, supra note 13, § 9.8.
\item \textsuperscript{135} See id. § 3.1.
\item \textsuperscript{136} See Sloan, supra note 35, at 1474. (“It is alleged that ECHELON intercepts all major modes of signal transmission, including land-lines, high-frequency radio, microwave radio relay, communications satellites, subsea cables, and the Internet.”); see also Loeb, supra note 42, at A3 (citing reports that estimate that the ECHELON system captures up to 3 billion communications each day).
\item \textsuperscript{137} USSID 18, supra note 13, § 7.1.
\item \textsuperscript{138} Id. (“Generic or general terms or phrases must be substituted for the identity (e.g. ‘U.S. firm’ for the specific name of a U.S. Corporation or ‘U.S. Person’ for the specific
semination of the U.S. person’s identity in a number of circumstances. For instance, section 7.2(c) allows a U.S. person’s name to be disseminated if the person’s identity is “necessary to understand the foreign intelligence information or assess its importance.” The section also includes a non-exhaustive list of situations that would satisfy this requirement. For example, section 7.2(c) provides that inadvertently acquired information regarding a U.S. person may be disseminated directly to domestic law enforcement agencies if the information indicates that the U.S. person is somehow involved in criminal activity. This can occur despite the fact that no warrant was issued to authorize the initial surveillance responsible for acquiring the incriminating evidence from the unsuspecting and otherwise constitutionally protected U.S. person.

The Fourth Amendment has yet to be extended to prevent such a situation. The issue is difficult to resolve because those who have standing to challenge such surveillance are unaware that they were initially targeted for criminal investigation based on information gained through warrantless surveillance of their international phone calls by the NSA. The current controversy involving the secret directive issued by President Bush may bring these issues before the Supreme Court in the near future. Should this occur, many key issues will be presented, and the next generation of Fourth Amendment rights may be defined.

name of a U.S. Person). Files containing the identities of U.S. persons deleted from SIGINT reports will be maintained for a maximum period of one year . . .

139 Id. § 7.2.
140 Id. § 7.2(c).
141 Id.
142 USSID 18, supra note 13, § 7.2(c)(4). Information about a U.S. person can be kept and disseminated if “[t]he information is evidence that the individual may be involved in a crime that has been, is being, or is about to be committed, provided that the dissemination is for law enforcement purposes.” Id.
143 See id.
144 Although FISA requires the government to notify criminal defendants when it seeks to use, against the defendant, information obtained through electronic surveillance, this requirement is limited to information obtained pursuant to a FISA warrant and also does not apply unless the government seeks to introduce the evidence at trial. The statute does not require the government to inform the defendant about information used only to initiate a criminal investigation. If the government does not seek to introduce the FISA evidence at trial, then it presumably may keep that evidence secret. Moreover, this requirement also only applies in situations where FISA is applicable. Thus, lawfully warrantless non-FISA foreign surveillance is not subject to this limitation. See FISA, 50 U.S.C. § 1806(c)–(d) (2000 & Supp. III 2003).
Perhaps the controversy also will cause legal policymakers at the NSA to reexamine the application of the current minimization procedures expressed in USSID 18. If so, one question that the Court should consider, when determining whether to allow the dissemination of information without a warrant, is the degree to which those procedures should take into account the reasonableness of one’s expectation of privacy. Because the scope of the Fourth Amendment’s protection is based largely on the reasonableness of one’s subjective expectation of privacy, it seems to follow that individuals should be able to take affirmative technological steps such as the use of encrypted Internet telephony that would provide them with heightened constitutional protection against unwarranted invasion.

III. ENCRYPTED VOICE OVER INTERNET PROTOCOL, CRYPTANALYSIS, AND THE TERRITORIAL LIMITS OF CONSTITUTIONAL RIGHTS

A. Encrypted VoIP

As technology advances, the ability of individuals to protect their privacy against undesired intrusion is growing. In recent years, an increasing number of people are using Internet telephony—also known as Voice over Internet Protocol (“VoIP”)—instead of traditional telephone services for their international telecommunications. VoIP converts analog voice communications into a compressed digital data format that is then transferred from computer to computer over regular Internet protocol data networks. This enables computer users to speak to one another via the Internet using their existing Internet connections, often at no additional cost. Because the data is converted into a digital form prior to transmission, efforts are increasing to bring about widespread use of data encryption methods to protect these

---

146 VoIP usage is on the rise, and major corporations are beginning to invest large sums in its development. In September 2005, eBay, Inc. purchased Skype Technologies, S.A. for $2.6 billion. Skype Technologies is currently the world leader in Internet telephony, with 54 million customers and projected revenue of more than $200 million in 2006. Although criticized by some as a risky investment by eBay, the move certainly demonstrates a strong expectation that use of Internet telephony will continue to grow significantly in coming years. See Jonathan Krim, EBay’s Skype Risk Is a Calculated One, WASH. POST, Sept. 22, 2005, at D1.
148 See id.
communications from eavesdropping en route. For instance, Skype Technologies, one of the world’s leading VoIP providers, utilizes a 256-bit Advanced Encryption Standard (“AES”) encryption algorithm that many experts believe to be functionally unbreakable. Difficulties are posed, however, when users of one service attempt to communicate with users of another.

Today, VoIP encryption is still in its infancy, with widespread inter-service usage being hindered by the difficulty in standardization of VoIP protocols and the unwillingness of some providers to offer open architectures that would allow different encryption algorithms to negotiate between communication endpoints. These barriers are slowly being eroded by the efforts of privacy advocates and philanthropic cryptographic experts who are working to adapt popular open-source cryptosystems for widespread distribution and usage. Thus, despite initial compatibility difficulties, the use of encrypted

---


150 See David S. Bennahum, Can They Hear You Now?, Slate, Feb. 19, 2004, http://www.slate.com/id/2095777/ (quoting the National Institute of Science and Technology as stating that “it would take a computer using present-day technology ‘approximately 149 thousand-billion (149 trillion) years to crack a 128-bit AES key’”). Skype’s 256-bit standard offers an even greater level of security. Id.

151 Skype uses a proprietary protocol that is not compatible with many other standards, such as Session Initiation Protocol (“SIP”) and Inter-Asterisk eXchange Protocol (“IAX”); therefore, users of other providers are often unable to communicate with users on the Skype network. See Brian Livingston, Beware Skype’s Hype; Focus on SIP-Compliant Internet Calling Instead, eWeek, Dec. 1, 2003, at 64 (“Skype isn’t compatible with SIP. You could wake up one day to a nightmare in which some of your offices have adopted SIP while others have downloaded Skype. Users couldn’t rely on the incompatible services to call one another.”); see also Skype’s the Limit, Info. Age, Sept. 21, 2005, http://www.information-age.com/article/2005/september/skypes_the_limit (discussing the prospect of adding VoIP service to Google Talk and stating that “Google favours using IP telephony technology from start up SIPphone, which is compatible with the Vonage service but not Skype.”).

152 See Antonopoulos & Knape, supra note 149; Livingston, supra note 151, at 64; Skype’s the Limit, supra note 151.

153 Most recently, the famous cryptographer Phillip Zimmermann announced a new encrypted VoIP program known as Zfone. In 1991, Zimmermann gained international acclaim from privacy advocates when he developed Pretty Good Privacy (“PGP”), an encryption program used to encrypt e-mail transmissions as well as stored data. Zimmermann distributed the software for free, even publishing the source code on the Internet, in order to allow peer scrutiny of the program. PGP was rumored to be unbreakable, even by the NSA, and Zimmermann subsequently became the target of an extensive three-year federal criminal investigation for alleged violations of U.S. export restrictions on dual-use cryptographic technology. See Ronald Bailey, Code Blues, Reason, May 1994, at 36; see also John E. Dunn, Encryption Guru Returns with VoIP Software, PCWorld, July 27, 2005, http://www.pcworld.com/news/article/0,aid,122000,00.asp; Phil Zimmermann’s Home Page, Background, http://www.philzimmermann.com/EN/background/index.html (last visited Mar. 28, 2006).
VoIP is beginning to spread and will soon become the standard for all voice-over-Internet communications.

Although VoIP communications originally could be freely captured and overheard by anyone possessing the requisite technical knowledge,\(^{154}\) today’s encrypted VoIP conversations are practically indecipherable, even by the most sophisticated professionals.\(^{155}\) The NSA and CSS together form the world’s premier cryptographic agency, employing the most advanced cryptanalytic capabilities in existence.\(^{156}\) Through various means, the agency is able to decipher a significant percentage of the encrypted communications it captures each day via ECHELON and other means.\(^{157}\) However, the decryption process involves additional steps that raise constitutional concerns.\(^{158}\)

The decryption of encrypted VoIP communications requires the agency to take numerous additional steps in order to understand the information they have acquired.\(^{159}\) Although ECHELON may cast a wide net, capturing most electronic communications transmitted worldwide, the NSA/CSS must employ extraordinary measures before any encrypted VoIP communication can be understood and analyzed.\(^{160}\) This raises questions about the reasonable expectations of U.S. citizens employing these technologies and the extent to which the Constitution, through the application of the Fourth Amendment, should permit the government to use information gained through the frustration of those expectations.

\(^{154}\) See Niall Magennis, *Skills Development*, Network News, Mar. 31, 1999 (available on LexisNexis) (“Security is critical to the future of VoIP because it is remarkably easy to listen in on current VoIP conversations using a protocol analyzer.”).

\(^{155}\) See Bennahum, *supra* note 150.

\(^{156}\) Nat’l Sec. Agency/Cent. Sec. Serv., *supra* note 24.


\(^{158}\) In Part IV of this Article, I argue that the government’s use of the extraordinary measures necessary to crack encrypted VoIP violates the reasonable expectation of privacy held by protected persons under the Fourth Amendment. See *infra* notes 192–232 and accompanying text.

\(^{159}\) See Max Schireson, *Decoding the Complexities of Cryptography*, PC Wk., Jan. 10, 1994, at 84 (discussing several methods of cryptanalysis).

\(^{160}\) The term “extraordinary means” is used here to refer to the use of electronic or other resources which perform high-speed processing that exceeds the capabilities of human beings.
B. Cracking Encrypted VoIP Through Cryptanalysis

In order to provide a background for the cryptanalysis debate, it is helpful to define some of the basic terminology in the field. There is a distinct difference between decryption through cryptanalysis and through non-cryptanalytic means. The term “cryptanalysis” refers to methods through which encrypted messages are decrypted without having access to the password or passphrase that allows those messages to be deciphered.\textsuperscript{161} In other words, this involves cracking the encryption itself.\textsuperscript{162} In comparison, non-cryptanalytic methods involve learning or “stealing” the relevant passwords or passphrases.\textsuperscript{163}

Cryptographers use many techniques to break codes directly. Although a detailed discussion of such cryptanalytic techniques is beyond the scope of this Article, it is useful to discuss briefly several cryptanalytic techniques in order to distinguish them from the more invasive non-cryptanalytic methods discussed in Part III.C. One form of cryptanalysis involves attacking the encryption algorithm directly. Because computer algorithms are used to encrypt data, structural weaknesses in those algorithms may be exploited to decipher messages encrypted using that method.\textsuperscript{164} Many of the most popular encryption algorithms utilized today are open-source and have been tested extensively for the types of structural weaknesses that plagued some earlier encryption standards.\textsuperscript{165} Although the structural integ-

\textsuperscript{161} BBC.co.uk, Basic Cryptanalysis, http://www.bbc.co.uk/dna/h2g2/alabaster/A613135 (last visited Apr. 5, 2006).
\textsuperscript{162} See id.
\textsuperscript{163} See id.
\textsuperscript{164} An algorithm is a set of instructions which is performed to accomplish a certain task. In the case of encryption software, the encryption algorithm performs a set of recurring operations to scramble data into an unintelligible form. Because of the recurring nature of these operations, a weakness in the design of the algorithm can produce patterns which can be exploited to decrypt data which has been encrypted using that method. See Scott Fluhrer, Itsik Mantin, & Adi Shamir, Weaknesses in the Key Scheduling Algorithm of RC4 (unpublished manuscript), available at http://www.drizzle.com/~aboba/IEEE/rc4_kaproc.pdf (last visited Mar. 30, 2006) (exposing a major flaw in Wired Equivalent Privacy (“WEP”) that stemmed from the fact that its key scheduling algorithm caused the same keys to be repeated often and at predictable intervals); see also Rik Farrow, Wireless Security: Send in the Clowns?, NETWORK MAG., Sept. 1, 2003, at 54 (discussing WEP’s vulnerability); Bob Walder, Networks Focus; Cryptography, COMPUTER WKLY., Nov. 25, 2003, at 50 (providing an explanation of public and private key encryption systems).
\textsuperscript{165} Open-source programs are assumed to be well-tested because anyone in the world is free to examine them; however, some experts caution that open-source availability does not necessarily guarantee security. See Gary McGraw & John Viega, Practice Safe Software Coding, INFO. SECURITY, Sept. 2001, at 62 (“One common fallacy is to believe that open-source software is likely to be secure, because its availability will lead to people performing
rity of such algorithms is sound, their open-source nature means that there is no secret as to their operation. Therefore, the only thing standing in the way of sophisticated decryption efforts is the strength of the key that controls the operation of the cipher.

Cryptographers use many methods to decipher encryption keys. For example, encrypted texts may be subjected to a number of techniques, such as “brute force” attack, differential cryptanalysis, or known-plaintext and chosen-plaintext attacks. All are means of deciphering messages without having access to the passphrase used to decode them. In theory, virtually all ciphers can be broken by “brute force” or other cryptanalytic means. However, given the myriad of possible keys and passphrases that could be used, these methods often prove to be too time consuming for practical application. For example, the National Institute of Science and Technology estimates that it would take a standard computer approximately 149 trillion years to break even a 128-bit AES key, which is currently half the length of the AES keys used to encrypt Skype’s VoIP transmissions.

Even assuming the vastly superior computational abilities of the NSA, standard decryption via conventional cryptanalytic means would be very inefficient. Although the specific methods of the NSA are

---

166 Kerckhoffs’ Law stands for the proposition that, regardless of the sophistication of the data encryption algorithm, one should never rely on the secrecy of the algorithm alone to maintain the security of encrypted data. Because of the nature of algorithms, it is reasonable to assume that the details of the algorithm’s operation are known to whomever is attempting to decrypt encrypted ciphertext. Security is provided not by the secrecy and complexity of the algorithm, but rather by the secrecy and complexity of the key. See BBC.co.uk, supra note 161.

167 See id.

168 The simplest form of cryptanalysis is known as a “brute force attack.” This method involves bombarding an encrypted message with every possible key or passphrase in an attempt to decipher the code. Data Encryption Essentials; Software Security, SOFTWARE WORLD, Sept. 1, 2005, at 15.

169 See Max Schireson, Decoding the Complexities of Cryptography, PC Wk., Jan. 10, 1994, at 84 (providing a description of differential cryptanalysis).


172 See Bennahum, supra note 150 (discussing the incredible amount of time necessary to perform a successful brute force attack on a message encrypted using 128-bit AES encryption).

173 See id.

174 See id.
not publicly known, it can be assumed that the agency uses such methods only as a last resort. Direct cryptanalysis is unnecessary if the NSA is able to determine a person’s passphrase. This could be achieved though a variety of means. In addition to the more forceful “rubber-hose” methods, there are a number of non-cryptanalytic techniques that the NSA could employ to learn a suspect’s passphrase.

C. Non-Cryptanalytic Means of Cracking Encrypted VoIP

Given the difficulty of applying direct cryptanalytic methods to defeat the use of modern encryption programs, the U.S. government has developed other means of deciphering these conversations. Such non-cryptanalytic methods include social engineering, signals intelligence (electronic surveillance), phishing, site spoofing (pharming), and keystroke logging. In late 2001, the Federal Bureau of Investigation (the “FBI”) was reported to have developed its own key-

---


176 See Elizabeth Clark, Illuminating Magic Lantern, Network Mag., Feb. 1, 2002, at 18 (discussing the FBI’s keystroke-logging Trojan Horse virus known as “Magic Lantern”).

177 Social engineering is a broad term that encompasses many other forms of non-cryptanalytic tactics such as phishing and pharming. Social engineering involves exploiting the naiveté of unsophisticated computer users to gain knowledge of passphrases and other personal data. See Security Dictionary, Info. Age, May 11, 2005, available at http://www.information-age.com/article/2005/may/security_dictionary.

178 Phishing is a tactic often used by hackers whereby an e-mail is sent to various users claiming to be from a well-known financial organization. Such e-mails often claim that a problem has arisen that requires the recipient to log in to a website purportedly administered by the financial organization. When the person logs into the fake site, he or she ends up providing his or her password and login details to criminals who then use the information to gain access to the user’s actual account. See Chris Green, Data Business; ‘Tis the Season to Beware Phishing Scams, Computing, Dec. 15, 2005, at 38.

179 Site spoofing, also known as “pharming,” is often performed in conjunction with phishing. Site spoofing involves manipulation of the Domain Name System to direct Internet traffic to imposter websites. These imposter sites appear to be the exact same as the legitimate company being spoofed. When customers attempt to log in to these sites their user IDs, passwords, credit card numbers, or other personal data is sent directly to the criminals running the site. See Catherine Sanders Reach, Pharming & Other New Hacker Scams, L. Tech. News, May 2005, at 46 (offering an explanation of “pharming”).

stroke-logging virus.\textsuperscript{181} The program, known as “Magic Lantern,” works like the standard keystroke-logging Trojan horse viruses traditionally used by hackers.\textsuperscript{182} The FBI surreptitiously uploads its keystroke-logging software onto the computers of those it seeks to surveil.\textsuperscript{183} Once installed, this program allows the FBI to record every keystroke that users type into the infected computer.\textsuperscript{184} When the suspect types in his or her passphrase, this information is captured and then may be used to decipher every communication or file that is encrypted using the same phrase.\textsuperscript{185}

Although the FBI must obtain a warrant in order to install such programs on computers within the United States, the NSA is not required to obtain a warrant before installing similar programs on the computers of non-U.S. persons abroad.\textsuperscript{186} As a result, U.S. persons contacting foreign persons abroad via e-mail or Internet telephony may have those communications compromised despite the use of encryption.

D. U.S. Legal Restraints on the Use of Cryptanalytic and Non-Cryptanalytic Tactics on Non-U.S. Persons Outside the United States

Under U.S. law, there are virtually no legal restraints on the ability of the NSA to use cryptanalytic or non-cryptanalytic tactics against non-U.S. persons outside the United States.\textsuperscript{187} It has long been recognized that the U.S. Constitution does not extend its protections outside U.S. borders, except with respect to U.S. persons.\textsuperscript{188} For example, in 1990, in \textit{United States v. Verdugo-Urquidez}, the Supreme Court held that the Fourth Amendment does not place any limits on the ability of U.S. government agents to perform even physical searches of the homes of aliens outside the United States.\textsuperscript{189} A natural extension of this decision is that no warrant is required for even the most intrusive

\begin{flushleft}
\textsuperscript{182} Christopher Woo & Mirada So, \textit{The Case for Magic Lantern: September 11 Highlights the Need for Increased Surveillance}, 15 \textsc{Harv. J.L. \\& Tech.} 521, 524 (2002).
\textsuperscript{183} See id.
\textsuperscript{185} See id.
\textsuperscript{187} See supra notes 51–144 and accompanying text.
\textsuperscript{189} 494 U.S. at 274–75.
\end{flushleft}
electronic invasions of foreign computers by government agents.\textsuperscript{190} In light of the length of time it takes to perform actual cryptanalysis to break ciphers and the lack of legal restrictions in this area, it can be assumed that the NSA widely employs methods similar to Magic Lantern and has installed Trojan horse software on many computers of interest throughout the world.

Given the NSA’s exceptional cryptanalytic resources and the absence of domestic legal restraints on the agency’s use of non-cryptanalytic methods on aliens outside the United States, even the most private international VoIP calls of U.S. citizens probably may be overheard, despite the use of reasonable steps to maintain privacy. Even American citizens who have taken every reasonable precaution to avoid eavesdropping—by using encrypted VoIP technology—may have their conversations decrypted and overheard by the NSA as a result of the use of invasive non-cryptanalytic techniques against the NSA’s foreign contact. This is although the use of such techniques clearly would be illegal if conducted directly against the U.S. person without a warrant.\textsuperscript{191} Situations such as this violate the reasonable expectations of American citizens who use encrypted VoIP technology. When information acquired through these means is then used by the government to initiate a criminal investigation against a U.S. person, a court should find that the Fourth Amendment has been violated.

IV. THE CONSTITUTIONAL OVERBREADTH OF USSID 18 § 7.2(c)(4) AS APPLIED TO THE ENCRYPTED VOIP CONVERSATIONS OF U.S. PERSONS

A. The Fourth Amendment and Reasonable Expectations of Privacy

The Fourth Amendment places its protections largely in the hands of individuals. It guarantees that protected persons will not be subjected to warrantless government invasions of their private lives if they take reasonable measures to ensure their privacy.\textsuperscript{192} The warrant requirement of the Fourth Amendment extends to situations where an objectively reasonable and legitimate expectation of privacy ex-

\textsuperscript{190} See id.

\textsuperscript{191} The Fourth Amendment requires the government to obtain a warrant before using invasive methods of cryptanalysis in most cases. See United States v. Scarfo, 180 F. Supp. 2d 572, 577–78 (D.N.J. 2001) (explaining that the FBI needed a warrant to install a keystroke-logging program on a suspect’s computer).

\textsuperscript{192} See Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).
Although one is not entitled to claim privilege over matters left open to the world, people may expect that private conversations will remain free from unwarranted government surveillance if reasonable measures have been taken to keep those conversations from being overheard. If such measures have been taken, then a reasonable expectation of privacy exists, and those conversations may not be surveilled absent probable cause and a warrant demonstrating that proof has been made to that effect.

The Supreme Court has established a two-part analysis that is used to determine whether a particular area is entitled to Fourth Amendment protection. First, the person must have “manifested a subjective expectation of privacy” in that area. It would be difficult to argue that this prong is not satisfied in the case of either encrypted or unencrypted VoIP because it can be assumed that most people hold a subjective expectation that their private telephonic conversations will not be overheard by unknown third parties. This subjective expectation is manifested even more clearly when users choose to protect their conversations through encryption.

Second, the expectation of privacy must be one that “society is willing to recognize as legitimate.” The Supreme Court has generally adopted a rights-based approach to handling this second criterion, finding that one must have a right of privacy in the disputed area enforceable outside of the Fourth Amendment to claim a legally justifiable expectation of privacy. Society has long recognized the

194 See Katz, 389 U.S. at 352 (holding that even a telephone conversation taking place in a public telephone booth is entitled to Fourth Amendment protection, provided that the individual closes the door).
195 See id. at 357 (“‘Over and again this Court has emphasized that the mandate of the Fourth Amendment requires adherence to judicial processes,’ and that searches conducted outside the judicial process, without prior approval by judge or magistrate, are per se unreasonable under the Fourth Amendment . . . .”) (quoting United States v. Jeffers, 342 U.S. 48, 51 (1951)) (footnote omitted).
196 Id. at 361 (Harlan, J., concurring); see also Bond v. United States, 529 U.S. 334, 338 (2000) (“Our Fourth Amendment analysis embraces two questions. First, we ask whether the individual, by his conduct, has exhibited an actual expectation of privacy; that is, whether he has shown that ‘he [sought] to preserve [something] as private. . . .’ Second, we inquire whether the individual’s expectation of privacy is ‘one that society is prepared to recognize as reasonable.’”) (quoting Smith v. Maryland, 442 U.S. 735, 740 (1979)) (footnote omitted).
197 Ciraolo, 476 U.S. at 211.
198 Id.; see also Katz, 389 U.S. at 361 (Harlan, J., concurring).
legitimacy of one’s expectation of privacy during telecommunications. For example, both FISA and the ECPA make it a felony to engage in nonconsensual telephonic eavesdropping without a warrant.\textsuperscript{200} VoIP is essentially a telephone call that is made using alternative means. Accordingly, it is illogical to argue that society would be willing to accept phone conversations as legitimately private when conducted via traditional phone networks but somehow illegitimate and unprotected when conducted via secure Internet telephony.\textsuperscript{201} Thus, both prongs of the test are satisfied. Accordingly, VoIP conversations should be protected by the Fourth Amendment, and the government should be required to obtain a warrant prior to undertaking targeted surveillance of such conversations.\textsuperscript{202}


\textsuperscript{201} Initially, courts had been unwilling to recognize a reasonable expectation of privacy in calls made using cordless telephones due to the ease with which they could be inadvertently monitored. See McKamey v. Roach, 55 F.3d 1236, 1239–40 (6th Cir. 1995). In 1994, Congress passed the Communications Assistance for Law Enforcement Act, which extended the wiretapping prohibitions of Title III of the Omnibus Crime Control and Safe Streets Act of 1968, making them applicable to eavesdropping on cordless telephones as well as land-based phones. Communications Assistance for Law Enforcement Act, Pub. L. No. 103-414, § 202, 108 Stat. 4279, 4290–91 (1994) (codified at 18 U.S.C. §§ 2510–2511 (2000 & Supp. III 2003)). Even before Congress extended Title III’s protections, the situation posed by portable phones was entirely distinguishable from the case of both traditional and encrypted VoIP. Although neighbors using similar phones could inadvertently over hear cordless telephone calls, eavesdropping on traditional VoIP conversations requires intentional efforts by someone with an uncommon level of computer knowledge and skill. In the case of encrypted VoIP, not only are such conversations immune from casual or inadvertent eavesdropping, but intentional surveillance also is rendered ineffective by the level of encryption employed. Only the most sophisticated technicians with access to state-of-the-art equipment and extraordinary computational resources would be able to decrypt such communications. Thus, due to the almost unparalleled security of VoIP communications, the Fourth Amendment certainly should extend to protect users’ expectations that their encrypted VoIP conversations will not be surveilled by the government without a warrant.

\textsuperscript{202} Although courts generally have refused to recognize a general right to privacy for web surfing and other public activities on the Internet, the issue of whether the government may seize private person-to-person Internet communications en route is a different matter entirely. See Mitchell Waldman, Annotation, \textit{Expectation of Privacy in Internet Communications}, 92 A.L.R. 5TH 15, § 5 (2001). Courts have already recognized a person’s reasonable expectation that private e-mails and phone conversations will not be intercepted by the government en route without a warrant. E.g., United States v. Monroe, 52 M.J. 326, 330 (C.A.A.F. 2000) (“The transmitter of an e-mail message enjoys a reasonable expectation that police officials will not intercept the transmission without probable cause and a search warrant.”) (citing United States v. Maxwell, 45 M.J. 406, 417 (C.A.A.F. 1996)); United States v. Long, 61 M.J. 539, 546 (N-M. Ct. Crim. App. 2005) (“[W]hile the e-mails may have been monitored for purposes of maintaining and protecting the system from malfunction or abuse, they were subject to seizure by law enforcement personnel only by disclosure as a
Although it is clear that U.S. persons are protected from warrantless government surveillance targeting their VoIP conversations, U.S. persons are not currently protected from situations where such conversations are surveilled indirectly by the government during the otherwise lawful warrantless surveillance of non-U.S. persons abroad. When such a situation occurs, and information to and from U.S. persons is collected without a warrant, the Fourth Amendment should still apply, and the reasonable expectations of protected persons should be respected.

B. Are Some Expectations More Reasonable than Others?

Arguably, a U.S. citizen’s expectation of privacy in international communications has never been more reasonable. According to estimates, it would take a computer trillions of years to decipher a message encrypted using an encryption standard that employs a key length half of that currently used by Skype.\(^\text{203}\) Consequently, encrypted VoIP users can be certain not only that their communications are virtually immune from random eavesdropping, but that even the NSA would find it difficult—perhaps even impossible—to surveil those conversations purposefully, even with the extraordinary computational resources at their disposal.\(^\text{204}\) Because encrypted VoIP is so secure, it stands to reason that one’s expectation of privacy in such communications is much higher than it is with almost any other form of communication. Because Fourth Amendment protection is based largely on the reasonableness of one’s expectations, it would seem that using encrypted VoIP should provide U.S. citizens with the highest level of Fourth Amendment protection.\(^\text{205}\)

Some scholars disagree with this assessment, contending instead that the use of encryption can never provide a reasonable expectation

---

\(^{203}\) See Bennahum, supra note 150.

\(^{204}\) See id.

of privacy. In a 2001 article, Professor Orin Kerr argues that encryption can never offer a reasonable expectation of privacy for Fourth Amendment purposes because the Fourth Amendment limits only the acquisition of materials, not the process used to analyze the materials already in the government’s possession. This argument presupposes that information in the hands of the government has always come into its possession pursuant to some sort of warrant, plain view, or other constitutionally permissible means. It fails to consider the situation posed by the lawful warrantless surveillance conducted daily by U.S. intelligence agencies on foreign persons abroad. Lawful international signals intelligence operations result in an enormous amount of data coming into the possession of the government without a warrant each day. Under Professor Kerr’s analysis, which finds that encryption itself offers no reasonable expectation of privacy, the government would be free to do what it pleases with the data collected even if it was obtained through warrantless surveillance of U.S. citizens. Once the data was lawfully in the possession of the government, the Fourth Amendment’s protections could never be triggered.

This argument is untenable in light of the Supreme Court’s Fourth Amendment jurisprudence. The issue of whether an item is constitutionally protected is determined based solely on whether the person claiming protection had manifested a subjective expectation of privacy in that item, and whether that expectation is one which society is willing to recognize as reasonable. It is the reasonableness of one’s expectations that controls, not the location of the challenged evidence. The fact that a piece of evidence is already in the hands of the government is irrelevant to the constitutional analysis and simply begs the question.

---

206 See Kerr, supra note 199, at 532.
207 See id. at 505 (“[E]ncryption cannot create Fourth Amendment protection because the Fourth Amendment regulates government access to communications, not the cognitive understanding of communications already obtained.”).
208 See Loeb, supra note 42, at A3.
209 Professor Kerr’s argument sets up an artificial all-or-nothing scenario. Under his view, either all encryption creates a reasonable expectation of privacy, or no encryption creates such an expectation. See Kerr, supra note 199, at 524 (“[I]f encryption can ‘lock’ a communication and create a reasonable expectation of privacy, then every kind of encryption, ranging from Pig Latin . . . to the strongest public key encryption, must trigger the same Fourth Amendment protection.”).
210 Katz, 389 U.S. at 361 (Harlan, J., concurring).
211 See id. at 352 (majority opinion).
Professor Kerr’s analysis uses a plain-view rationale to explain why review of items already in the possession of the government should not be subject to any further Fourth Amendment limitations. This argument, however, ignores the fact that just because an item may be readily seen by the government does not necessarily mean that the item is in plain view. The simple fact that a piece of encrypted ciphertext may be seen by police does not mean that its contents are readily visible. In order to truly see the underlying message, government agents must employ tactics and resources beyond mere human analysis in order to bring the decrypted message’s contents into view. When encrypted data has come into the possession of the government without a warrant, and in violation of the reasonable expectations of a protected person, the decryption of that data should require a warrant.

The Supreme Court’s jurisprudence in this area makes it clear that the “plain view” doctrine requires materials seized in warrantless searches to have been readily visible to the naked eye without the use of extraordinary or superhuman means. In 2001, in *Kyllo v. United States*,

---

212 See generally Kerr, supra note 199. To support his claim that the Fourth Amendment does not limit the efforts of law enforcement once materials are already in their possession, Professor Kerr offers an oversimplification of the decryption process likening it to taping together torn papers, solving riddles, understanding Pig Latin, or reading a doctor’s messy handwriting. See id. at 520, 521, 524. To be sure, the examples offered by Professor Kerr would not be entitled to protection; however, this is not because the “encrypted” items are in the hands of the government, but rather because they may be interpreted through human effort and are therefore in plain view. Torn papers may be taped together, foreign languages may be interpreted, and messy handwriting may be readily understood without technological assistance. Cryptanalysis of computer-generated encryption, however, requires the use of advanced computational resources that vastly surpass human capacity.

213 Professor Kerr compares encrypted ciphertext to a riddle and points out that, regardless of the difficulty of a particular riddle, one could never expect a Fourth Amendment expectation of privacy with respect to its meaning. Id. at 522–24. Again, this analogy fails to recognize the difference between what can be seen or decrypted using human effort and what can be seen only by using extraordinary means beyond natural human capacity. See id. at 522.

214 See Florida v. Riley, 488 U.S. 445, 450–51 (1989) (holding that a defendant did not have a reasonable expectation of privacy in a greenhouse, the contents of which were clearly visible from the sky). In *Florida v. Riley*, where police peered inside the defendant’s greenhouse from a helicopter hovering 400 feet above the greenhouse, the Court discussed the altitude of the police helicopter at length, and the fact that the greenhouse’s contents were visible with the naked eye was crucial to the Court’s finding that the area was not protected by the Fourth Amendment. See id. at 450. Likewise, the police in *California v. Ciraolo* used a small plane to hover 1000 feet above the defendant’s backyard; had they needed special X-ray goggles or the use of a supercomputer to view the marijuana plants growing in the backyard, presumably the Court would have found that such efforts re-
the Court specifically rejected the argument that high technology could be used to view the contents of protected areas not readily seen by the naked eye.\footnote{533 U.S. 27, 34–35 (2001).} The \textit{Kyllo} Court noted that a contrary approach would leave the Fourth Amendment’s protection “at the mercy of advancing technology.”\footnote{Id. at 35. \textit{See generally} Raymond Shih Ray Ku, \textit{The Founders’ Privacy: The Fourth Amendment and the Power of Technological Surveillance}, 86 \textit{Minn. L. Rev.} 1325 (2002) (discussing the constitutional restraints on the government’s ability to use technology to enhance surveillance capabilities).} Specifically, the Court ruled in \textit{Kyllo} that the government may not use thermal imaging technology to learn about the contents of a protected space without a warrant.\footnote{Kyllo, 533 U.S. at 40.} A natural extension of this holding is that the government is also prohibited from using technology to learn about the contents of a protected communication without a warrant.\footnote{Professor Kerr offers a hypothetical involving a terrorist named Lex Luthor who places an ad in a newspaper containing an obvious and easily broken code detailing a plot to blow up a New York City subway station. \textit{See Kerr, supra note 199, at 519.} If one simply rips up a piece of paper or utilizes a simple encryption standard that can be broken through basic human effort, such as the simple substitution cipher referenced in Professor Kerr’s Lex Luthor hypothetical, then not even the fiercest privacy advocate would argue that a reasonable expectation of privacy exists. \textit{See Kerr, supra note 199, at 519.} To be sure, no one could reasonably claim an expectation of privacy in a newspaper advertisement. However, if a U.S. citizen is communicating with a friend telephonically—an area long recognized by society as legitimately private—and that person utilizes a military-grade encryption standard, thus rendering their conversations indecipherable to all but the NSA, then that person is entitled to Fourth Amendment protection because the expectation of privacy is reasonable. The fact that the government is already in possession of the encrypted information is irrelevant to the inquiry.} This is not to say that the government may not use computers to decrypt data that is already in its possession pursuant to a lawfully issued warrant. The Fourth Amendment does not stand for the proposition that a person’s reasonable expectation of privacy will \textit{never} be violated by the government, only that a warrant is required to do so.\footnote{See U.S. Const. amend. IV.} Such information may be decrypted not because it is already in the possession of the government—as asserted by Professor Kerr—but rather because it has come to be in its possession pursuant to a warrant issued after a showing of probable cause. In instances where conversations have come into the possession of the government without a war-

\begin{thebibliography}{99}
\item \textit{Ciraolo}, 476 U.S. at 215 (“[I]t is unreasonable for respondent to expect that his marijuana plants were constitutionally protected from being observed with the naked eye from an altitude of 1,000 feet.”).
\item \textit{Id.} at 35. \textit{See generally} Raymond Shih Ray Ku, \textit{The Founders’ Privacy: The Fourth Amendment and the Power of Technological Surveillance}, 86 \textit{Minn. L. Rev.} 1325 (2002) (discussing the constitutional restraints on the government’s ability to use technology to enhance surveillance capabilities).
\item \textit{Kyllo}, 533 U.S. at 40.
\end{thebibliography}
rant, the reasonable expectations of the person surveilled must be respected.

To be sure, the government should not be required to determine a person’s protected status prior to all signals collection efforts. Such an assessment would be impossible in the case of inadvertently acquired information. A person’s reasonable expectations should simply be respected to the fullest extent practicable, and information collected from a U.S. person without a warrant should never be used to initiate general domestic criminal investigations against them unless truly exigent circumstances are presented.

Professor Kerr states that “the Fourth Amendment is not a roving privacy machine,” but in many ways, it is.220 The Supreme Court has long held that “the Fourth Amendment protects people, not places.”221 This protection travels with a person wherever he or she goes, and it covers all situations where a legitimate expectation of privacy can be held.222 The Supreme Court has made it clear that it is the reasonableness of a person’s expectation of privacy, not the geographic location of the conversation in question, that determines whether or not a conversation is protected.223 American citizens do not lose their Fourth Amendment rights simply because they set foot outside the United States; likewise, their conversations do not become fair game once the electrons transmitting them pass beyond U.S. borders.224

220 See Kerr, supra note 199, at 506.
221 Katz, 389 U.S. at 351.
222 The Supreme Court has rejected the argument that an individual’s Fourth Amendment protection is limited to certain physical locations. Instead, according to the Court, the protection travels with the individual, and even phone calls made from public telephones may be protected if they are conducted in a manner that prevents them from being casually overheard. See id. at 352.
223 See id.
224 Although the Supreme Court has never had occasion to hold that the Fourth Amendment extends to protect American citizens from the acts of U.S. agents abroad, it seems likely that the Court would do so if the issue were ever brought before it. See generally United States v. Conroy, 589 F.2d 1258, 1264 (5th Cir. 1979) (“The Fourth Amendment not only protects all within our bounds; it also shelters our citizens wherever they may be in the world from unreasonable searches by our own government.”). The Circuit Courts of Appeals are almost unanimous on the issue, as demonstrated by their application of the joint venture doctrine. The joint venture doctrine states that the Fourth Amendment does not apply to searches conducted against U.S. persons abroad unless the searches are performed by U.S. agents or by foreign agents who are acting in close association with U.S. agents. See United States v. Morrow, 537 F.2d 120, 139 (5th Cir. 1976) (stating that the exclusionary rule may be invoked if U.S. agents are involved in an unlawful search conducted by foreign officials overseas); see also United States v. Behety, 32 F.3d 503, 510 (11th Cir. 1994) (stating that the Fourth Amendment may apply to a foreign search “if the foreign officials conducting the search were actually acting as agents for their American coun-
C. Redrafting USSID 18 § 7.2(c)(4) to Respect Reasonable Expectations of Privacy

The reasonable expectation of privacy held by those using encrypted VoIP should afford them the highest level of protection available under the Fourth Amendment. Although such Fourth Amendment protection should not prevent the government from analyzing inadvertently acquired information, it should certainly prevent it from using such information against protected persons except in cases of emergency or situations where serious national security concerns are involved.

Under most circumstances, USSID 18 minimizes the impact of NSA surveillance on U.S. persons. Under the directive, when information pertaining to a U.S. person is inadvertently acquired, either it must be destroyed or the U.S. person’s identity must be obscured or redacted from all reports. However, USSID 18 section 7.2(c)(4) allows information obtained without a warrant to be kept and disseminated to law enforcement if it evinces any criminal conduct on the part of the inadvertently surveilled U.S. person. No consideration is
given to the reasonableness of the communicant’s expectation of privacy, and no limitations are expressed regarding the types of offenses that may be revealed.\footnote{228}{See id.}

Under the provision as it is currently written, evidence that an American citizen may have committed a misdemeanor could properly be disseminated to police for local criminal investigation.\footnote{229}{See id.} There is no differentiation or qualification regarding the seriousness of the offense revealed.\footnote{230}{See id.} Without any limitation on the type of “criminal” information that can be turned over to law enforcement, this provision represents a violation of the Fourth Amendment rights of those surveilled.\footnote{231}{See id.} A reasonable limitation must be placed on this dissemination power, limiting it to situations where grave national security or other emergency situations are presented. Most of the other exceptions listed under USSID 18 section 7.2(c) require some form of exigent circumstance to exist before a U.S. citizen’s identity may be divulged.\footnote{232}{See USSID 18, supra note 13, § 7.2(c). All but two of the exceptions listed under USSID 18 section 7.2(c) require the existence of circumstances which raise serious national security or public safety concerns. Subsection 1 provides an exception if the information indicates that the U.S. person may be an agent of a foreign power. Id. § 7.2(c)(1). Subsection 2 allows disclosure if it appears the U.S. person may be “engaged in the unauthorized disclosure of classified information.” Id. § 7.2(c)(2). Subsection 3 allows disclosure if the U.S. person is involved in international drug trafficking. Id. § 7.2(c)(3). Subsection 5 allows disclosure if the information indicates that a “U.S. person may be the target of hostile intelligence activities of a foreign power.” Id. § 7.2(c)(5). Subsection 6 allows disclosure if the information is pertinent to a threat to the safety of an organization or person. Id. § 7.2(c)(6). The only two exceptions listed under USSID 18 section 7.2 that do not raise potentially serious consequences for non-disclosure are: (1) subsection 7, which allows disclosure of the identities of senior executive branch officials; and (2) subsection 4, which allows disclosure of information that indicates any act of criminal behavior, with no limitation on the type or seriousness of the criminal conduct that may trigger the exception. See id. § 7.2(c)(4), (7).}

**Conclusion**

Although the NSA’s surveillance capabilities have grown considerably in recent years, so have the means through which citizens may affirmatively protect their own privacy. New forms of encrypted Internet telephony are offering Americans the ability to provide unparalleled security for their international telecommunications. Such methods were not generally available to the public when the current version
of USSID 18 was drafted in 1993. Even before the advent of encrypted VoIP, courts had recognized that U.S. citizens held a reasonable expectation that their e-mails and communications would not be captured en route by the government without a warrant. Now that encryption technology is becoming more widely available, U.S. citizens are enjoying an extraordinary expectation of privacy, the reasonableness of which is unprecedented in the field of communication.

The NSA is perhaps the most important force protecting the United States from foreign terrorism and other threats to national security. The information provided by the agency informs national security and foreign policy decisionmakers, thereby also playing a vital role in ensuring international peace and security. While the incredible value of this agency cannot be overstated, neither can the risks posed by its vast capabilities. The broad scope of the agency’s vigilant efforts has the potential to threaten the legitimate rights of American citizens, and appropriate checks must be in place.

FISA provides a well-established legal framework that has protected the rights of American citizens from unwarranted government surveillance since 1978. Although it appears that this framework recently may have been circumvented through a secret executive order, warrantless surveillance of Americans is nothing new. Gaps in our legal protections have existed since FISA’s enactment.

The NSA’s minimization procedures provide strong protection for the rights of U.S. citizens under most circumstances, but they allow breaches to occur in situations that are arguably the most crucial. Although the NSA is required to destroy information inadvertently obtained about U.S. citizens in most cases, the current minimization procedures allow the agency effectively to initiate criminal investigations by turning over such information to law enforcement if criminal conduct is revealed. This places Americans at risk of criminal prosecution resulting from warrantless eavesdropping on their private telecommunications. This should not be permitted. Although it may not be practicable for the NSA to obtain a warrant in every case where

---

233 See United States v. Jones, 149 F. App’x 954, 959 (11th Cir. 2005); see also United States v. Monroe, 52 M.J. 326, 330 (C.A.A.F. 2000).

234 See Olmstead v. United States, 277 U.S. 438, 472–73 (1928) (Brandeis, J., dissenting) (providing a more fervent expression of this concept).


236 See Risen & Lichtblau, supra note 2, at A1.

237 See supra notes 51–144 and accompanying text.

238 See supra notes 51–144 and accompanying text.
information about U.S. citizens may be inadvertently acquired, the heightened expectation of privacy provided by encrypted Internet telephony should require additional limitations on what may be done with such information after it is acquired.

USSID 18 must be redrafted to forbid the use of inadvertently obtained information for the purpose of initiating criminal investigations against U.S. citizens unless exigent circumstances are presented. By disallowing the use of such information for these purposes, the government would be ensuring that the NSA stays focused on its primary mission—protecting the United States from terrorism and foreign intelligence operations—and not engaging in general criminal investigations domestically. Under the current directive, the NSA has an incentive to collect as much “inadvertently acquired” information as possible. If the possibility of using such information to initiate unrelated criminal investigations were removed, the agency would cease to have an incentive to collect information unrelated to its national security mission. This would provide the agency with an incentive to maintain its focus on foreign terrorism and counterintelligence, and it would curb the temptation to stray into unrelated matters more appropriately left to those charged with domestic law enforcement.

This solution would allow the NSA to protect U.S. national security, while also enabling American citizens to communicate with foreign acquaintances without fear. It would also have the benefit of restoring public confidence in the NSA, effectively combating the perception that the agency engages in frequent violations of the very rights it was created to defend.
OLD RULE, NEW THEORY: REVISING THE PERSONAL BENEFIT REQUIREMENT FOR TIPPER/TIPPEE LIABILITY UNDER THE MISAPPROPRIATION THEORY OF INSIDER TRADING

Abstract: Under the classical theory of insider trading, tipper/tippee liability may arise only when the tipper makes the relevant disclosure to obtain a personal benefit. Courts are divided, however, as to whether this personal benefit requirement applies to the misappropriation theory of insider trading. This Note argues that because the personal benefit requirement is severely flawed, courts should not impose it in misappropriation cases. Instead, courts adjudicating misappropriation cases should require that (1) the tipper was at least reckless as to whether he or she would either benefit personally or harm the information source by tipping, and (2) the tipper was at least reckless as to whether someone in the line of tippees would use the information to trade. This standard should be subject only to the tipper’s defense that the disclosure was made in a good faith attempt to prevent criminal activity reasonably certain to cause substantial physical or financial harm to others.

Introduction

Suppose that you, the CEO of Acme Corporation, disclose to your Vice President that your company plans to make a tender offer for Zen Corporation. You warn the Vice President that this information is sensitive and confidential and must not be discussed with anyone outside of the office. He agrees to keep the secret. Unbeknownst to you, however, the Vice President dislikes you and your company, plans to quit soon, and does not feel particularly loyal.

After work, the Vice President gets a haircut. During the haircut, the barber asks the Vice President whether Acme Corporation plans to buy any other companies soon. The Vice President knows the barber is an avid stock trader because the barber often talks about his investments. He also believes that the barber is probing for information with high trading value. The barber has mentioned that he and

---

1 For a set of facts similar to those provided in this hypothetical, see SEC v. Maxwell, 341 F. Supp. 2d 941, 943–45 (S.D. Ohio 2004).
his friends enjoy finding and then investing in acquisition targets, and every time he gives the Vice President a haircut, he goes out of his way to ask whether Acme Corporation plans to make any acquisitions in the near future.

The Vice President also knows that anyone who buys stock in Zen Corporation now would likely enjoy a large profit due to the upcoming offer. In addition, the Vice President knows that there is a substantial chance that leaking information about the tender offer would harm his company because leaking information about an upcoming acquisition may cause the acquisition to fall apart.

Nevertheless, the Vice President is tired of having to watch his words for a company he dislikes. Indifferent to the consequences, he tells the barber about the upcoming offer. He does not speak in order to bestow a gift upon the barber, who is not his friend. He also does not speak in order to obtain a better haircut, a better price, or a good reputation with the barber.² He simply does not feel like watching his words.

In fact, the barber was probing for information with high trading value. Knowing that the Vice President probably was not supposed to talk about the upcoming tender offer, the barber quickly tells his friends and they all use the information to buy stock in Zen Corporation. Zen Corporation’s stock price rises.

In addition, because the barber’s friends are not careful about whom they tell, rumors spread about an upcoming tender offer for Zen Corporation, eventually causing two more companies to join the bidding war. Ultimately, your company must abandon its contemplated offer because the bidding war has pushed the purchase price too high. Your company missed a perfect opportunity to expand its business. People learn that you told the Vice President about the upcoming offer and, as a result, your reputation is damaged. Meanwhile, the barber and his friends sell their stock in Zen Corporation, reaping millions in profits.

Despite the Vice President’s conscious disregard of a substantial risk that the barber would trade based on the information and that his disclosure would cause you and your company tremendous harm, some courts and authors would insist that he escape all federal insider

---

² See id. at 948 & n.2 (“[G]iven [the insider-tipper’s and barber-tippee’s] relative stations in life, any reputational benefit to [the insider-tipper] in the eyes of his barber is extremely unlikely to have translated into any meaningful future advantage. . . . ‘Surely it cannot be claimed that the purpose of the alleged disclosure was so [the insider-tipper] would receive a better haircut, a better appointment slot, a better price?’”).
trading liability. They reason that the Vice President sought no personal benefit in disclosing the information with which you entrusted him. This seems wrong, however. After all, your company is defrauded of the exclusive use of the information with which you entrusted the Vice President. Furthermore, the integrity of the securities markets is harmed as a result. What is the basis for the personal benefit requirement?

In 1983, in Dirks v. SEC, the U.S. Supreme Court held that where a corporate insider discloses material, nonpublic information to one who then uses that information to trade in the stock of the insider’s corporation, the corporate insider and the trader are not liable unless the tipper personally benefited from making the tip. The Court reasoned that where a tipper does not personally benefit, the tip does not constitute a breach of duty to the corporation’s shareholders. Absent such a breach, neither the tipper nor the tippee can be liable

---


4 See Yun, 327 F.3d at 1275; Ebaugh, supra note 3, at 288–93. Although one might try to argue that the Vice President sought the “benefit” of speaking freely, this is likely too trivial to meet the personal benefit standard. See Dirks v. SEC, 463 U.S. 646, 663–64 (1983) (identifying personal benefits of consequence for the requirement that the tipper intend to benefit personally from the tip, such as a pecuniary gain, an enhanced reputation, or the satisfaction of making a valuable gift to a relative or friend); Maxwell, 341 F. Supp. 2d at 948 (holding that there was no personal benefit where the tipper-insider tipped his barber because “Dirks requires an intended benefit of at least some consequence” and there was no evidence that the tipper-executive sought money, a reputational gain, or the satisfaction of giving a gift to the barber); SEC v. Switzer, 590 F. Supp. 756, 766 (W.D. Okla. 1984) (holding that there was no personal benefit where a father-tipper made the disclosure for the purpose of making child care arrangements).

5 463 U.S. at 662. Information is material if there is a substantial likelihood that a reasonable investor would consider it important when deciding how to invest. See Basic Inc. v. Levinson, 485 U.S. 224, 231–32 (1988). To be nonpublic, information must be specific and more private than general rumor. United States v. Mylett, 97 F.3d 663, 666 (2d Cir. 1996). For purposes of this Note, a “tipper” is a person who discloses material, nonpublic information to another person. If the recipient of that information uses it by trading or passing it along to others, that recipient is a “tippee.” Depending on the circumstances, both the tipper and the tippee may be held liable for insider trading. See Dirks, 463 U.S. at 662.

6 Dirks, 463 U.S. at 662.
for insider trading, in part because breach of duty is an important “limiting principle” that protects tippers and tippees from unreasonable enforcement actions by the Securities and Exchange Commission (the “SEC”).

The Court decided the case under the so-called “classical theory” of insider trading, which posits that a person who owes a fiduciary duty to a corporation’s shareholders must not use material, nonpublic information about the corporation to trade in the corporation’s stock unless the person first discloses the information to the shareholders.

Subsequently, in 1997, in United States v. O’Hagan, the Supreme Court adopted an additional theory of insider trading—the misappropriation theory—under which the Vice President in the example above could be prosecuted. Similar to the classical theory, the misappropriation theory was also designed to protect investors. The misappropriation theory, however, differs from the classical theory in a crucial way: the fraud victim is not a shareholder of the traded corporation, but rather the source of the information used for the trade. In other words, misappropriation liability arises when a trader or tipper breaches a fiduciary duty to the source of the information, rather than a duty to shareholders of the corporation whose stock is bought or sold.

Since O’Hagan, this fundamental difference has caused confusion as to which aspects of the classical theory should apply to misappropriation cases. For instance, it is unclear whether a misappropriation...

---

7 Id. at 662, 664 & n.24 (suggesting that the SEC has sent mixed signals to the public regarding who will be subject to its enforcement actions, and that legal limitations are therefore necessary).

8 Id. at 653–61. For the purpose of brevity, cases decided under the classical theory of insider trading will hereinafter be referred to as “classical cases.”

9 See United States v. O’Hagan, 521 U.S. 642, 650 (1997). The Vice President also could likely be prosecuted under SEC Rule 14e-3. See 17 C.F.R. § 240.14e-3(a) (2005) (prohibiting trading on the basis of material, nonpublic information regarding an upcoming tender offer that the trader knows, or has reason to know, was acquired from an insider of the offeror or issuer, or someone working on their behalf); id. § 240.14e-3(d) (prohibiting disclosure when it is reasonably foreseeable that the disclosure is likely to result in a trade that violates Rule 14e-3(a)).


11 See id.

12 See id.

13 See SEC v. Sargent, 229 F.3d 68, 77 (1st Cir. 2000) (noting disagreement as to whether the personal benefit requirement for tipper/tippee liability should apply to misappropriation cases); Donna M. Nagy, Reframing the Misappropriation Theory of Insider Trading Liability: A Post-O’Hagan Suggestion, 59 Ohio St. L.J. 1223, 1287–310 (1998) (arguing that despite dicta in O’Hagan suggesting the contrary, disclosure to the source in misap-
tor’s disclosure to the source of the intention to trade is sufficient to negate liability in the same way that disclosure to shareholders negates liability in classical cases.\textsuperscript{14} Another unresolved issue is whether the misappropriation theory precludes tipper/tippee liability where the tipper does not seek to benefit from the tip.\textsuperscript{15} \textit{Dirks} established that such preclusion clearly exists under the classical theory, but courts are divided as to whether this is also true under the misappropriation theory.\textsuperscript{16}

Part I of this Note reviews the common-law development of insider trading laws under section 10(b) of the Securities Exchange Act and SEC Rule 10b-5 promulgated thereunder.\textsuperscript{17} In doing so, this Part examines the two theories of insider trading: the classical and misappropriation theories.\textsuperscript{18} Part II focuses specifically on the liability of tippers and tippees for insider trading.\textsuperscript{19} This Part examines the circumstances in which insider trading liability may arise when a person who holds material, nonpublic information discloses that information to one who then trades.\textsuperscript{20} Part II also gives special attention to the requirement, under \textit{Dirks}, that the tipper personally benefit by making the tip.\textsuperscript{21} Part III argues that courts should not impose the personal benefit requirement in cases brought under the misappropriation

\textsuperscript{14} See \textit{O’Hagan}, 521 U.S. at 654–55. The \textit{O’Hagan} Court stated that disclosure to the information source prior to trading undermines the claim of deception of the information source and thus also does not constitute a SEC Rule 10b-5 violation of fraud in securities trading. \textit{Id.} at 655. This was merely dicta, however, and a compelling argument can be made that deception still remains even when such disclosure is made. \textit{See id.} at 647–48, 654–55 (demonstrating that the Court’s assertion was merely dicta because the defendant in the case did not disclose to the information source his intent to trade); Nagy, \textit{supra} note 13, at 1287–310 (arguing that deception remains even in the face of disclosure to the source). For instance, the investors with whom the misappropriator trades are arguably still deceived. Nagy, \textit{supra} note 13, at 1287–310 (arguing that courts faced with cases involving such disclosure could find that the investors with whom the misappropriator trades are still deceived).

\textsuperscript{15} See \textit{Sargent}, 229 F.3d at 77 (noting disagreement among courts).

\textsuperscript{16} See \textit{Dirks}, 463 U.S. at 662 (requiring a personal benefit in classical cases); \textit{Yun}, 327 F.3d at 1275 (requiring a personal benefit in misappropriation cases); SEC v. \textit{Willis}, 777 F. Supp. 1165, 1172 n.7 (S.D.N.Y. 1991) (requiring no personal benefit in misappropriation cases).

\textsuperscript{17} See infra notes 25–80 and accompanying text.

\textsuperscript{18} See infra notes 25–80 and accompanying text.

\textsuperscript{19} See infra notes 81–150 and accompanying text.

\textsuperscript{20} See infra notes 81–150 and accompanying text.

\textsuperscript{21} See infra notes 81–150 and accompanying text.
theory.\textsuperscript{22} Instead, this Part explains, courts should require that (1) the tipper was at least reckless as to whether he or she would either benefit personally or harm the information source by tipping, and (2) the tipper was at least reckless as to whether someone in the line of tippers would use the information to trade.\textsuperscript{23} This standard should be subject only to the tipper’s defense that the tipper made the disclosure in a good faith attempt to prevent criminal activity reasonably certain to cause substantial physical or financial harm to others.\textsuperscript{24}

I. The Development of Insider Trading Prohibition Under Section 10(b) and Rule 10b-5

Section 10(b) of the Securities Exchange Act of 1934, and SEC Rule 10b-5 promulgated thereunder, provide the primary basis for courts’ proscription of insider trading.\textsuperscript{25} Together, they create a broad prohibition of fraud in connection with securities trades.\textsuperscript{26} The scope of the prohibited conduct has evolved over decades through interpretations by the courts and the SEC, and through this evolution, two theories of insider trading have emerged: the classical and misappropriation theories.\textsuperscript{27}

A. The Classical Theory

Initially, insider trading was proscribed through what is now known as the classical theory.\textsuperscript{28} In its early stages, its scope was unclear.\textsuperscript{29} Government prosecutors attempted to require anyone in possession of material, nonpublic information about a corporation either

\textsuperscript{22} See infra notes 151–270 and accompanying text.
\textsuperscript{23} See infra notes 151–270 and accompanying text.
\textsuperscript{24} See infra notes 151–270 and accompanying text.
\textsuperscript{25} Securities Exchange Act of 1934 § 10(b), 15 U.S.C. § 78j(b) (2000); 17 C.F.R. § 240.10b-5 (2005); 3 Thomas Lee Hazen, The Law of Securities Regulation § 12.17, at 492 (5th ed. 2005) (identifying Rule 10b-5 as the primary basis for the prohibition of insider trading). In the special situation where the information used for trading relates to a tender offer, the trade is also subject to Rule 14e-3, which proscribes trading on the basis of material, nonpublic information regarding an upcoming tender offer if the trader knows, or has reason to know, that the information has been acquired from an insider of the offeror or issuer, or someone working on their behalf. 17 C.F.R. § 240.14e-3(a) (2005).
\textsuperscript{26} See 15 U.S.C. § 78j(b); 17 C.F.R. § 240.10b-5.
\textsuperscript{28} See id.
to disclose that information to the marketplace or refrain from trading in that corporation’s stock.\textsuperscript{30} Whether courts would ultimately sanction such a broad rule, however, remained to be seen.\textsuperscript{31}

In 1961, the SEC laid the groundwork for this broad rule in \textit{In re Cady, Roberts & Co.}\textsuperscript{32} In \textit{Cady, Roberts}, the directors of a public company decided to reduce the company’s dividends.\textsuperscript{33} Soon after the decision was made, one of the directors telephoned a broker to communicate the upcoming reduction.\textsuperscript{34} The broker then sold 7000 shares of the company’s stock before the company publicly announced the dividend cut to the marketplace.\textsuperscript{35} The public announcement of the cut caused the stock price to fall, and therefore the broker avoided significant losses by selling prior to the announcement.\textsuperscript{36}

As part of the settlement between the brokerage firm and the SEC, the SEC explained how the broker’s sales violated Rule 10b-5.\textsuperscript{37} The SEC stated that insider trading liability is premised on a relationship that provides access to information intended only for a corporate purpose, as well as the “inherent unfairness” involved where a party takes advantage of the information gained from the special relationship while knowing it is unavailable to those with whom he deals.\textsuperscript{38} Thus, the broker violated Rule 10b-5 when he took advantage of his access to this material, nonpublic information for trading purposes knowing that the investing public remained unaware of it.\textsuperscript{39}

In 1968, the U.S. Court of Appeals for the Second Circuit endorsed the SEC’s broad theory.\textsuperscript{40} In \textit{SEC v. Texas Gulf Sulphur Co.}, the Second Circuit stated that \textit{anyone} who possesses material, nonpublic information about a company must either disclose that information to

\begin{itemize}
\item \textsuperscript{30} See \textit{SEC v. Tex. Gulf Sulphur Co.}, 401 F.2d 833, 848 (2d Cir. 1968) (adopting this broad requirement).
\item \textsuperscript{31} See \textit{id.}, cert. denied, 394 U.S. 976 (1969) (demonstrating the U.S. Supreme Court’s decision not yet to resolve the matter).
\item \textsuperscript{32} See 40 S.E.C. 907, 910–18 (1961).
\item \textsuperscript{33} \textit{Id.} at 909.
\item \textsuperscript{34} \textit{Id.}
\item \textsuperscript{35} \textit{Id.}
\item \textsuperscript{36} \textit{Id.} at 909–10.
\item \textsuperscript{37} \textit{Cady, Roberts}, 40 S.E.C. at 907–08, 910–18.
\item \textsuperscript{38} \textit{Id.} at 912.
\item \textsuperscript{39} See \textit{id.} at 910–18.
\item \textsuperscript{40} See \textit{Tex. Gulf Sulphur Co.}, 401 F.2d at 848.
\end{itemize}
the investing public or abstain from trading in that company’s stock. The court reasoned that this rule protected the justifiable expectation of the marketplace that all investors enjoy relatively equal access to material information.

In 1980, however, in Chiarella v. United States, the U.S. Supreme Court rejected this “equal access” rule. In Chiarella, which remains the law today, the Court significantly narrowed the scope of the classical theory. The Court held that under Rule 10b-5, a duty either to disclose information or abstain from trading arises only from a specific fiduciary relationship or similar relationship of trust and confidence. In the context of the classical theory, this means that a person cannot be held liable for insider trading in a certain corporation’s stock unless the person owes a fiduciary duty to that corporation’s shareholders. In other words, to be liable under the classical theory, a person must be an insider or tippee of an insider of the traded corporation. With this principle in mind, the Chiarella Court reversed the conviction of an employee of a financial printer who, while on the job, learned of several upcoming mergers and subsequently bought stock in the target corporations. Because the financial printer was hired by the acquiring corporations rather than the targets, the employee owed no derivative fiduciary duty to the shareholders of the target corporations. There-

41 Id. One should note, however, that the defendants in the case were officers, directors, and employees of the traded company, and therefore this broad language was probably dicta as applied to others. See id. at 839.
42 Id. at 848.
44 See id. at 228–29; see also O’Hagan, 521 U.S. at 652 (favorably discussing Chiarella); Dirks v. SEC, 463 U.S. 646, 654–58 (1983) (favorably citing Chiarella).
46 See id.
47 See id. For example, if a CEO of a drug company learns of medical tests showing that the company’s flagship product causes severe cancer as a side-effect—a revelation that would surely make the company’s stock price fall upon public disclosure—the CEO must either disclose that information to the company’s shareholders or refrain from selling his or her stock in the company. See id. But if an outsider learns the same information—for example, he sees a copy of the medical report that the CEO accidentally left on the subway—the outsider is free to sell any stock he owns in the company without penalty because he owes no fiduciary duty to the company’s shareholders. See id. Furthermore, in this situation he is not a tippee of the CEO because the CEO only inadvertently imparted the information, without any intent to benefit from the disclosure. See Dirks, 463 U.S. at 662. Typical “insiders” include persons such as officers and directors, and may also include accountants, lawyers, consultants, and other people to whom the corporation divulges information solely for business purposes. Id. at 655 n.14.
49 Id. at 232–33.
fore, the employee’s trading in the targets’ stock without disclosure of the upcoming mergers to the targets’ shareholders could not give rise to insider trading liability under Rule 10b-5.50

B. The Misappropriation Theory

In response to the Supreme Court’s restriction of the scope of the classical theory in Chiarella, the government began to prosecute insider trading cases under an alternate theory: the misappropriation theory.51 The government posited that the specific fiduciary duty required by Chiarella could be one owed not only to a corporation’s shareholders, but also to a source of information.52 Thus, the government asserted that a person who steals information and uses it for trading purposes, in breach of a fiduciary duty to the information source, also should be liable under section 10(b).53 The Chiarella Court had left open the issue of whether such a misappropriation theory was viable.54

On the one hand, several circuit courts agreed with the government’s position and adopted the misappropriation theory.55 For instance, in 1983, the Second Circuit in United States v. Newman affirmed the 10b-5 insider trading convictions of employees of an investment banking firm who misappropriated information from the firm for trading purposes.56 The employees conveyed the information to traders and shared the profits reaped from purchasing the stock of upcoming merger targets.57 The court found the employees liable because they breached a fiduciary duty to the investment bank and the bank’s clients, from whom they stole the information.58

50 Id.
52 Id.
53 Id.
54 O’Hagan, 521 U.S. at 662. In his dissent in Chiarella, Chief Justice Burger advocated the misappropriation theory as the proper basis for liability in that case. 445 U.S. at 240, 244–45 (Burger, J., dissenting).
55 See, e.g., SEC v. Cherif, 933 F.2d 403, 410 (7th Cir. 1991); SEC v. Clark, 915 F.2d 439, 453 (9th Cir. 1990); United States v. Newman, 664 F.2d 12, 16–18 (2d Cir. 1981), aff’d, 722 F.2d 729 (2d Cir. 1983).
56 Newman, 664 F.2d at 16.
57 Id. at 15.
58 Id. at 16–18.
On the other hand, in 1995 the Fourth Circuit rejected the misappropriation theory in United States v. Bryan.\textsuperscript{59} The court reasoned that the theory would hold misappropriators liable absent deception, despite the fact that deception is a requirement for section 10(b) liability.\textsuperscript{60} And even if the misappropriation theory did require deception, the court reasoned, such deception would not occur “in connection with” a purchase or sale of securities, as section 10(b) requires.\textsuperscript{61} The requisite connection did not exist, the court reasoned, because the person deceived was an information source who did not necessarily have “some connection to, or some interest or stake in,” a securities trade.\textsuperscript{62}

In 1997, the U.S. Supreme Court in United States v. O’Hagan settled this circuit split by explicitly adopting the misappropriation theory.\textsuperscript{63} James O’Hagan, a partner at a law firm, learned that one of his firm’s clients planned to make a tender offer for another company.\textsuperscript{64} Prior to the public announcement of the offer, O’Hagan bought significant quantities of the target company’s stock and call options.\textsuperscript{65} After the public announcement, he sold them for a profit of more than $4.3 million.\textsuperscript{66} The trial court convicted O’Hagan of insider trading, money laundering, and mail fraud.\textsuperscript{67}

The Supreme Court upheld the insider trading conviction under the misappropriation theory.\textsuperscript{68} Justice Ginsburg, writing for the majority, opined that a fiduciary who receives information from a principal violates Rule 10b-5 when the fiduciary deceptively breaches a duty of loyalty and confidentiality to the principal by (1) using the information, without permission, to trade in securities, while (2) pretending not to do so.\textsuperscript{69}

The Court took pains to reject the criticisms raised by the Fourth Circuit in Bryan and the Eighth Circuit in O’Hagan.\textsuperscript{70} The Court em-

\textsuperscript{59} 58 F.3d 933, 952 (4th Cir. 1995).
\textsuperscript{60} Id. at 949; see Santa Fe Indus., Inc. v. Green, 430 U.S. 462, 473–76 (1977) (requiring deception for Rule 10b-5 liability).
\textsuperscript{61} Bryan, 58 F.3d at 949–50.
\textsuperscript{62} Id. at 950.
\textsuperscript{63} See 521 U.S. at 650.
\textsuperscript{64} Id. at 648.
\textsuperscript{65} Id. at 647.
\textsuperscript{66} Id. at 648.
\textsuperscript{67} Id. at 648–49.
\textsuperscript{68} See O’Hagan, 521 U.S. at 650.
\textsuperscript{69} Id. at 652, 654.
\textsuperscript{70} See id. at 654–56; United States v. O’Hagan, 92 F.3d 612, 620, 622 (8th Cir. 1996) (rejecting the misappropriation theory on the grounds that it fails the deception and “in
phasisized that under the misappropriation theory it was adopting, deception of the information source, not merely a breach of duty owed to the source, is required for liability. In this way, the Court reasoned, the misappropriation theory satisfies section 10(b)’s requirement of deception. Furthermore, the Court noted that this deception occurs “in connection with” a securities trade, as required by section 10(b), because the deception and securities trade coincide. They coincide because the fraud occurs when, without disclosure to his or her principal, the misappropriator uses the information to trade in securities. Thus, the Court reasoned, the theory is consistent with the text of section 10(b).

The Court also indicated that it was deriving the scope of the misappropriation theory from common-law principles of agency. The Court referred to the information source as a “principal” multiple times, and while discussing the requirements for misappropriator liability, the Court cited to the Restatement (Second) of Agency. Thus, the Court implied that courts should look to these agency principles when clarifying gray areas in the future.

In summary, the misappropriation theory is a viable alternative to the classical theory. While the classical theory applies to individuals who breach a fiduciary duty to the shareholders of the traded corporation, the misappropriation theory applies to individuals who breach a duty to the source of the information.

II. LIABILITY OF TIPPERS AND TIPPEES UNDER SECTION 10(B) AND RULE 10B-5

A person can be held liable for insider trading under Rule 10b-5 even if that person does not personally trade in stock; courts and the
SEC rules also permit liability under certain circumstances when a person communicates information to another person who then trades. The specific scope of tipper/tippee liability depends in part on whether the case is brought under the classical or misappropriation theory.

A. Classical Theory

In 1983, in Dirks v. SEC, the U.S. Supreme Court established the modern requirements for tipper/tippee liability under the classical theory. Ronald Secrist, a former officer of an insurance company, told Raymond Dirks, an investment analyst, that the insurance company was engaged in significant fraud. While investigating these allegations, Dirks revealed to some of his clients information about the fraud that he obtained from the insurance company’s employees. Some of these clients then sold their stock in the insurance company based on this information. Although Dirks’s investigation induced the public exposure of the insurance company’s fraud, the SEC nevertheless censured Dirks for insider trading violations under Rule 10b-5. On appeal, the U.S. Court of Appeals for the District of Columbia Circuit upheld the judgment against Dirks.

The Supreme Court, however, reversed the judgment against Dirks. The Court held that where a tippee receives information from a corporate insider, the tippee inherits the insider’s duty either to disclose that information to the corporation’s shareholders or to abstain from trading and tipping only if two requirements are met: (1) the insider breached a fiduciary duty to the shareholders by disclosing the information to the tippee, and (2) the tippee knew, or

---


82 See United States v. O’Hagan, 521 U.S. 642, 651–53 (1997) (explaining that the fraud victim in misappropriation cases is the source of the information, as opposed to classical cases where the fraud victim is a shareholder of the traded corporation). Compare Dirks, 463 U.S. at 662 (requiring a personal benefit to the tipper for tipper/tippee liability in classical cases), with SEC v. Willis, 777 F. Supp. 1165, 1172 n.7 (S.D.N.Y. 1991) (requiring no personal benefit for tipper/tippee liability in misappropriation cases).

83 See 463 U.S. at 660, 662.
84 Id. at 649.
85 Id.
86 Id.
87 Id. at 650–52.
88 Dirks, 463 U.S. at 652.
89 Id.
should have known, that such a breach occurred. The Court reasoned that a breach of duty requirement is necessary, in part, to provide a “guiding principle” for those market participants who wish to avoid insider trading liability. Otherwise, the Court reasoned, potential defendants would be unfairly forced to rely on the reasonableness of the SEC’s litigation strategy.

The Court reasoned further that an insider’s disclosure to a tippee constitutes a breach of duty only when the insider makes the disclosure for an improper purpose. The purpose is improper, the Court emphasized, only when the insider personally benefits from the disclosure. Such a benefit can come in the form of a pecuniary gain, reputational benefit, or benefits from making a gift to a relative or friend. Deriving this personal benefit requirement from In re Cady, Roberts & Co., the Court justified the requirement by noting that a major purpose of the Securities Exchange Act was to eliminate the idea that corporate officers may treat inside information as part of their compensation packages. The Court acknowledged, however, that it is not always easy to determine whether a corporate insider has gained a personal benefit from the tip.

Thus, the Court’s first step in its analysis was to determine whether Secrist and the other insurance company employees, the tippers, breached a duty to the insurance company’s shareholders by disclosing information to Dirks, the tippee. This turned on whether Secrist and the other employees obtained a personal benefit from the disclosures. The Court found that no such benefit existed. The Court emphasized that the tippers merely sought to expose fraud—Secrist and the employees believed that disclosure to Dirks was the best way to uncover the corporate wrongdoing because other efforts

90 Id. at 659–61.
91 Id. at 664.
92 Id. at 664 n.24 (suggesting that the SEC has sent mixed signals to the public regarding who will be subject to its enforcement actions, and therefore legal limitations are necessary).
93 Dirks, 463 U.S. at 662.
94 Id.
95 Id. at 663–64.
96 Id. at 653 n.10, 662 (citing In re Cady, Roberts & Co., 40 S.E.C. 907, 912 n.15 (1961)).
97 Id. at 664.
98 Dirks, 463 U.S. at 665.
99 Id. at 667.
100 Id.
had “proved fruitless.”101 Thus, the Court concluded that the tippers breached no duty to the shareholders and consequently, Dirks could not be held liable as a tippee.102

The Court appeared to be particularly swayed by the public service value of Secrist’s and the other employees’ disclosures.103 As Justice Blackmun pointed out in his dissent, “[t]he Court justifies Secrist’s and Dirks’ action because the general benefit derived from the violation of Secrist’s duty to shareholders outweighed the harm caused to those shareholders.”104 The Court emphasized that the tippers exposed fraud and therefore likely prevented corporate wrongdoing from victimizing many more investors.105 Furthermore, the Court emphasized the need to protect tippers from liability for disclosure to analysts, given that these analysts serve the important purpose of collecting and analyzing information, as well as the fact that simultaneous disclosure to shareholders or the public is impracticable.106

The Court was unclear, however, as to whether the tipper must intend to benefit personally or actually benefit personally.107 In applying the Dirks benefit rule, circuit courts are likewise inconsistent.108 Given that the Dirks Court appeared to place primary importance on the tipper’s motive, it seems that the Court probably intended an intent-to-benefit test.109

Although the government typically has no trouble proving the existence of a personal benefit, this is not always the case.110 For instance, in 2004 in SEC v. Maxwell, the U.S. District Court for the Southern District of Ohio found that the SEC produced insufficient evidence to establish that a corporate insider’s disclosure to his barber created a per-

101 Id. at 667 & n.27.
102 Id. at 667.
103 See Dirks, 463 U.S. at 652 n.8, 667 & n.27 (emphasizing the defendant’s role in exposing fraud); id. at 676–77 (Blackmun, J., dissenting) (noting that the Court created the personal benefit requirement in the first place because the general benefit derived from the tips outweighed the harm caused to the corporation’s shareholders).
104 Id. at 676–77 (Blackmun, J., dissenting).
105 See id. at 652 n.8, 667 & n.27 (majority opinion) (emphasizing the defendant’s role in exposing fraud); id. at 676–77 (Blackmun, J., dissenting) (noting that the Court created the personal benefit requirement in the first place because the general benefit derived from the tips outweighed the harm caused to the corporation’s shareholders).
106 See id. at 658–59 (majority opinion).
107 See id. at 662–63, 667.
108 Compare Yun, 327 F.3d at 1274–75 (applying an intent-to-benefit test), with SEC v. Sargent, 229 F.3d 68, 77 (1st Cir. 2000) (applying an actual-benefit test).
109 See Dirks, 463 U.S. at 662, 667.
110 Ebaugh, supra note 3, at 281 (noting the general ease of proof).
sonal benefit.\textsuperscript{111} Similarly, in 1984, in \textit{SEC v. Switzer}, the U.S. District Court for the Western District of Oklahoma found that the SEC failed to prove a personal benefit.\textsuperscript{112} In that case, the tipper was a corporate insider who disclosed business information to his wife while observing a track meet.\textsuperscript{113} The disclosure was overheard by the tippee, Switzer, who was sunbathing behind the couple.\textsuperscript{114} Because the tipper made the disclosure merely for the purpose of informing his wife of his schedule and making childcare arrangements, and thus only inadvertently imparted the information to the tippee, the court concluded that the tipper did not personally benefit from the disclosure.\textsuperscript{115}

Thus, in summary, under the classical theory, a tipper and a trading tippee are both liable for insider trading when, without disclosing the information to the shareholders of the traded corporation, the tipper breaches a fiduciary duty to the shareholders by conveying the information to the tippee to obtain a personal benefit, and the tippee knows, or should know, that the breach occurred.\textsuperscript{116}

\textbf{B. Misappropriation Theory}

In addition to classical cases, courts have applied tipper/tippee liability in misappropriation cases.\textsuperscript{117} In this context, the tippee inherits the tipper’s duty to disclose or abstain from trading when the tipper breaches a fiduciary duty to the source of the information and the tippee knows, or has reason to know, that the tipper has breached that duty.\textsuperscript{118} Unlike tipper/tippee liability in the context of the classical theory, however, courts are divided as to whether a personal benefit to the tipper is required for liability in misappropriation cases.\textsuperscript{119}

The Supreme Court has not yet addressed this issue.\textsuperscript{120} In \textit{Dirks}, the Supreme Court required a personal benefit in a case brought under the classical theory, before the Supreme Court had endorsed the

\begin{footnotes}
\item\textsuperscript{111} 341 F. Supp. 2d 941, 948 (S.D. Ohio 2004).
\item\textsuperscript{112} 590 F. Supp. 756, 766 (W.D. Okla. 1984).
\item\textsuperscript{113} \textit{Id.} at 761, 766.
\item\textsuperscript{114} \textit{Id.} at 762.
\item\textsuperscript{115} \textit{Id.} at 766.
\item\textsuperscript{116} \textit{Dirks}, 463 U.S. at 659–62.
\item\textsuperscript{117} \textit{See Yun}, 327 F.3d at 1269–70; United States v. Libera, 989 F.2d 596, 600 (2d Cir. 1993); \textit{Willis}, 777 F. Supp. at 1169.
\item\textsuperscript{118} \textit{See Yun}, 327 F.3d at 1269–70; \textit{Libera}, 989 F.2d at 600; \textit{Willis}, 777 F. Supp. at 1169.
\item\textsuperscript{119} \textit{Compare Yun}, 327 F.3d at 1275 (requiring a personal benefit), \textit{with Willis}, 777 F. Supp. at 1172 n.7 (requiring no personal benefit).
\item\textsuperscript{120} \textit{See Sargent}, 229 F.3d at 77 (noting disagreement among lower courts).
\end{footnotes}
misappropriation theory.\textsuperscript{121} Nor did the Supreme Court decide the issue when it adopted the misappropriation theory in \textit{O’Hagan}, because \textit{O’Hagan} was not a tipper/tippee case; the misappropriator in \textit{O’Hagan} personally traded on the stolen information.\textsuperscript{122}

On the one hand, some courts explicitly or implicitly reject the personal benefit requirement for misappropriation cases.\textsuperscript{123} For instance, in 1991 in \textit{SEC v. Willis}, the U.S. District Court for the Southern District of New York explicitly noted in dicta that the misappropriation theory does not require a showing of a benefit to the tipper.\textsuperscript{124} The court reached the same conclusion in 1989 in \textit{SEC v. Musella}.\textsuperscript{125}

Similarly, in 1993 in \textit{United States v. Libera}, the Second Circuit implied that it would not require a personal benefit in misappropriation cases.\textsuperscript{126} In that case, the court affirmed the defendants’ convictions for insider trading and stated:

\begin{quote}
[T]he misappropriation theory requires the establishment of two elements: (i) a breach by the tipper of a duty owed to the owner of the nonpublic information; and (ii) the tippee’s knowledge that the tipper had breached the duty. We believe these two elements, without more, are sufficient for tippee liability.\textsuperscript{127}
\end{quote}

As the First Circuit observed in its 2000 decision in \textit{SEC v. Sargent}, the Second Circuit’s failure to mention a personal benefit in \textit{Libera} strongly suggests that the Second Circuit would not require such a benefit for tipper/tippee liability.\textsuperscript{128}

On the other hand, some courts do require a personal benefit for misappropriation cases, and several authors have argued in favor of this approach.\textsuperscript{129} At least one author has reasoned that the personal

\begin{footnotes}
\textsuperscript{121} See Dirks, 463 U.S. at 662; see also \textit{O’Hagan}, 521 U.S. at 650 (adopting the misappropriation theory in 1997, fourteen years after \textit{Dirks} was decided).


\textsuperscript{124} See 777 F. Supp. at 1172 n.7.

\textsuperscript{125} See 748 F. Supp. at 1038 n.4.

\textsuperscript{126} See \textit{Libera}, 989 F.2d at 600.

\textsuperscript{127} Id.

\textsuperscript{128} Sargent, 229 F.3d at 77; see \textit{Libera}, 989 F.2d at 600.

benefit requirement is needed to further the Dirks policy of protecting tippers from liability in the case of inadvertent or fraud-exposing disclosures.\textsuperscript{130} For instance, disclosures exposing fraud arguably promote the misappropriation theory’s goal of protecting the integrity of the securities market.\textsuperscript{131}

Some authors and at least one court have reasoned that a personal benefit should be required in misappropriation cases because the benefit is already required in classical cases, and courts should try to make the classical and misappropriation theories as similar as possible.\textsuperscript{132} In 2003 in SEC v. Yun, the Eleventh Circuit employed this reasoning when it held that in misappropriation cases, the tipper and tippee are not liable unless the tipper seeks to benefit from the tip.\textsuperscript{133}

In support of its opinion that a personal benefit should be required in misappropriation cases, the Yun court first noted the need to develop consistency in insider trading case law.\textsuperscript{134} In addition, the court emphasized the similarity of the tippee’s and tipper’s positions under both theories.\textsuperscript{135} The tippee is on notice under both theories that the tippee received confidential information through a breach of duty, and the choice of theory makes no difference as to potential liability or harm to investors if the tippee trades on the information.\textsuperscript{136} In addition, the tipper breaches a duty under both theories and the resulting harm to the marketplace is the same.\textsuperscript{137} Based on these similarities, the Yun court concluded that it would be nonsensical to treat a tipper or tippee differently under the misappropriation theory as compared to the classical theory.\textsuperscript{138}

The Yun court also advanced a more pragmatic reason for its goal of synthesis. The Yun court reasoned that separating the two theories would permit the SEC, and courts hearing misappropriation cases, to

\textsuperscript{130} See Ebaugh, supra note 3, at 288–93.
\textsuperscript{131} See id. at 292.
\textsuperscript{132} See Yun, 327 F.3d at 1275–77; Davis, supra note 3, at 294; Plotkin, supra note 3, at 5.
\textsuperscript{133} 327 F.3d at 1275–77. The Yun court did not address whether a personal benefit is required in cases brought under Rule 14e-3 because the case before it did not involve information about a tender offer. See id. at 1267–68 (describing the material, nonpublic information at issue, which related to the traded corporation’s unfavorable earnings); 17 C.F.R. § 240.14e-3 (2005) (applying only to information regarding a tender offer).
\textsuperscript{134} Yun, 327 F.3d at 1276.
\textsuperscript{135} Id. at 1276–77.
\textsuperscript{136} Id. at 1276.
\textsuperscript{137} Id. at 1277.
\textsuperscript{138} Id. at 1276–77.
ignore precedent under the classical theory whenever they saw fit.\textsuperscript{139} Because virtually all violations under the classical theory would also be violations under the misappropriation theory, the court reasoned, failing to synthesize the theories would provide the government with ample opportunity to exploit the looser misappropriation standards by trying all cases under the misappropriation theory.\textsuperscript{140} In the context of the personal benefit requirement, the court opined, such a tactic would unacceptably render the Supreme Court’s decision in \textit{Dirks} a “dead letter.”\textsuperscript{141}

Aside from its synthesis rationale, the \textit{Yun} court also advanced more technical reasons for imposing the personal benefit requirement in misappropriation cases.\textsuperscript{142} For instance, the court reasoned that requiring a personal benefit is necessary to ensure that liability arises only if the tipper engages in deception in connection with a securities trade, not merely a breach of duty.\textsuperscript{143} Without the personal benefit test, the court reasoned, a tipper could be liable even where the tipper does not intend that the disclosure will result in a trade.\textsuperscript{144}

Furthermore, the \textit{Yun} court reasoned, requiring a personal benefit is supported by language in \textit{O’Hagan}, because in that case the Supreme Court either “explicitly state[d] or implicitly assume[d]” a personal benefit requirement for misappropriation cases.\textsuperscript{145} For instance, the \textit{Yun} court noted \textit{O’Hagan}’s assertion that in misappropriation cases, a breach of duty occurs through a fiduciary’s “‘self-serving use of a principal’s information to purchase or sell securities,’” and that one who “‘pretends loyalty to the principal while secretly converting the principal’s information for personal gain dupes or defrauds the principal.’”\textsuperscript{146} The \textit{Yun} court reasoned that, because a personal benefit is required for liability of misappropriators who personally trade, as evidenced by this language in \textit{O’Hagan}, it would be “absurd” not to require it for tippers as well, since omitting the requirement would have the effect of holding tippers liable more readily than the traders.\textsuperscript{147}

\begin{flushleft}
\textsuperscript{139} \textit{Yun}, 327 F.3d at 1275–76, 1279.
\textsuperscript{140} \textit{Id.} at 1279.
\textsuperscript{141} \textit{Id.}
\textsuperscript{142} \textit{See id.} at 1278–79.
\textsuperscript{143} \textit{Id.} at 1278 & n.33.
\textsuperscript{144} \textit{Yun}, 327 F.3d at 1278 & n.34.
\textsuperscript{145} \textit{Id.} at 1279.
\textsuperscript{146} \textit{Id.} (quoting \textit{O’Hagan}, 521 U.S. at 652–54).
\textsuperscript{147} \textit{Id.}
\end{flushleft}
Finally, some courts have merely applied the personal benefit test, but failed to explain why the requirement should apply to misappropriation cases.\(^{148}\) For instance, in 2000 in *SEC v. Blackman*, the U.S. District Court for the Middle District of Tennessee stated in a misappropriation case that *Dirks* required the tipper to receive some benefit to hold the tippee liable.\(^{149}\) The court did not expound, however, on why the *Dirks* personal benefit test necessarily applies to misappropriation cases.\(^{150}\)

### III. Revising the Personal Benefit Requirement in Misappropriation Cases

The personal benefit requirement for insider trading violations is flawed because it protects tippers to a much greater extent than is supported by its underlying policy rationale.\(^{151}\) For this reason, courts should decline to extend the requirement to the misappropriation theory, and should instead apply a revised requirement that better promotes the policies underlying the theory.\(^{152}\) To do this, courts facing tipper/tippee misappropriation cases should require that (1) the tipper was at least reckless as to whether he or she would either benefit personally or harm the information source by tipping, and (2) the tipper was at least reckless as to whether someone in the line of tippees would use the information to trade.\(^{153}\) This standard should be subject only to the tipper’s defense that the tipper made the disclosure in a good faith attempt to prevent criminal activity reasonably certain to cause substantial physical or financial harm to others.\(^{154}\)

#### A. Quarantining the Personal Benefit Requirement

The personal benefit requirement is flawed because it protects tippers from liability to a much greater extent than its underlying policy rationale can support.\(^{155}\) Because of this flaw, and because courts

---

\(^{148}\) See, e.g., Gonzalez de Castilla, 184 F. Supp. 2d at 375; Blackman, 2000 WL 868770, at *6–8.


\(^{150}\) See id.

\(^{151}\) See infra notes 155–183 and accompanying text.

\(^{152}\) See infra notes 155–183 and accompanying text.

\(^{153}\) See infra notes 184–270 and accompanying text.

\(^{154}\) See infra notes 184–270 and accompanying text.

\(^{155}\) See SEC v. Maxwell, 341 F. Supp. 2d 941, 944–50 (S.D. Ohio 2004) (exculpating a tipper and tippee where the tippee used the information selfishly, thus demonstrating how the personal benefit requirement can protect tippers and tippees who produce no social
are not bound to extend the requirement to the misappropriation theory under existing Supreme Court precedent, courts should confine the requirement to the classical theory of insider trading.\(^\text{156}\)

The Court articulated the underlying policy rationales in 1983 in *Dirks v. SEC*, when the Supreme Court held that tipper/tippee liability cannot arise unless the tipper intends to benefit personally from the tip.\(^\text{157}\) The Court appeared to be particularly swayed by the public service value of the insider-tippers’ disclosures to the analyst-tippee, who subsequently exposed the corporation’s wrongdoing and also induced his clients to sell their stock.\(^\text{158}\) Instead of placing importance on the fact that the tippers’ selective disclosures resulted in sales that caused harm to the oblivious purchasers whose share values subsequently plummeted, the Court emphasized the tippers’ efforts to expose fraud and the important role analysts play in the marketplace.\(^\text{159}\) With these concerns in mind, the Court created a blanket requirement under the classical theory that the tipper intend to benefit personally in providing the tip.\(^\text{160}\)

Unfortunately, it seems that these policy concerns do not justify a blanket personal benefit requirement.\(^\text{161}\) It is first important to note benefit to offset the harm they cause to investor confidence); Regulation FD, 17 C.F.R. § 243.100–.103 (2005) (forbidding selective disclosure to analysts); Selective Disclosure and Insider Trading, 65 Fed. Reg. 51,716, 51,716–18 (Aug. 24, 2000) (adopting Regulation FD and discussing the need for prohibition of selective disclosure to analysts); Selective Disclosure and Insider Trading, 64 Fed. Reg. 72,590, 72,592–93 (proposed Dec. 28, 1999) (discussing the need for prohibition of selective disclosure to analysts); Donald C. Langevoort, *Investment Analysts and the Law of Insider Trading*, 76 Va. L. Rev. 1023, 1044–45 (1990) (critiquing arguments in favor of selective disclosure to analysts).

\(^{156}\) See United States v. O’Hagan, 521 U.S. 642, 650 (1997) (adopting the misappropriation theory without addressing tipper/tippee liability); *Dirks v. SEC*, 463 U.S. 646, 662 (1983) (adopting a personal benefit requirement in cases brought under the classical theory). \(^{157}\) See *Dirks*, 463 U.S. at 652 n.8, 658–59, 667 & n.27. \(^{158}\) See *id.* \(^{159}\) See *id.* at 667 n.27 (asserting that the harm to shareholders from the ultimate tippees’ trades is of little legal significance and noting that the tippers’ disclosures prevented the victimization of many more investors). \(^{160}\) See *id.* at 652 n.8, 658–59, 662, 667 & n.27. \(^{161}\) See *Maxwell*, 341 F. Supp. 2d at 944–50 (exculpating a tipper for disclosure to a self-serving non-analyst tippee due to a lack of a personal benefit to the tipper, thus demonstrating how the personal benefit requirement can protect tippers and tippees who produce no societal benefit to offset the harm caused to investor confidence); Regulation FD, 17 C.F.R. § 243.100–.103 (2005) (forbidding selective disclosure to analysts, thus demonstrating that selective disclosures such as tips, especially those made to analysts, harm investor confidence); Selective Disclosure and Insider Trading, 65 Fed. Reg. 51,716, 51,716–18 (Aug. 24, 2000) (adopting Regulation FD and discussing the need for prohibition of selective disclosure to analysts); Selective Disclosure and Insider Trading, 64 Fed. Reg. 72,590,
that tipping gives a distinct informational advantage to a few investors—in the case of disclosures to analysts, the analysts’ clients—who are likely to use the information to trade.\textsuperscript{162} This trading is in turn likely to affect adversely the confidence of investors who lack such preferential access to information from corporate insiders.\textsuperscript{163} For this reason, tipping that is likely to result in trading should only be permitted when other important legal or policy considerations are strong enough to outweigh this resulting harm.\textsuperscript{164}

With this point in mind, the personal benefit requirement is overly broad because it protects tippers and tippees in several instances where the benefits of the disclosure do not outweigh the harm.\textsuperscript{165} For instance, selective disclosures to analysts in particular do more harm than good.\textsuperscript{166} Such disclosures can create an incentive for analysts to skew their recommendations in favor of the issuer, in hopes of continued preferential access to information.\textsuperscript{167} Corporate insiders might even delay public announcements in order to improve their relationships with analysts through selective disclosure.\textsuperscript{168} For these very reasons, in 2000 the SEC promulgated Regulation FD, which provides that when an issuer discloses material, nonpublic information to an analyst, it must also disclose that information to the public.\textsuperscript{169}

In addition, even if the personal benefit requirement could be justified in the case of disclosures to analysts in particular, the personal benefit requirement would still be overly broad because it also

\textsuperscript{162} See Selective Disclosure and Insider Trading, 64 Fed. Reg. at 72,592 n.15 (citing Richard Frankel et al., \textit{An Empirical Examination of Conference Calls as a Voluntary Disclosure Medium}, 37 J. Acct. Res. 133 (1999) (indicating that selective disclosure to analysts allows certain individuals to profit from trading before the information is announced publicly)).


\textsuperscript{164} See id.


\textsuperscript{166} See Selective Disclosure and Insider Trading, 64 Fed. Reg. at 72,592–93; Langevoort, supra note 155, at 1044–45.

\textsuperscript{167} Selective Disclosure and Insider Trading, 64 Fed. Reg. 72,590, 72,592–93 (proposed Dec. 28, 1999); Langevoort, supra note 155, at 1041–42.

\textsuperscript{168} Selective Disclosure and Insider Trading, 64 Fed. Reg. 72,592.

\textsuperscript{169} 17 C.F.R. § 243.100–103 (2005).
protects disclosures to self-serving non-analysts. Arguably, disclosures to analysts could be justified because analysts serve the commendable purpose of gathering and analyzing information for others’ benefit. The personal benefit requirement, however, also protects disclosures to self-serving tippees who will use the information solely for their own benefit by trading. For instance, in 2004 in SEC v. Maxwell, the U.S. District Court for the Southern District of Ohio found that the SEC produced insufficient evidence to establish that a corporate insider’s disclosure to his barber, who personally traded, created a personal benefit. Rather than gathering and analyzing information for the benefit of the marketplace, the barber-tippee self-servingly used the information to trade, reaping almost $200,000 in profits. Yet, because the tipper did not benefit personally, the barber-tippee escaped liability. Thus, even if the personal benefit requirement could be justified in the narrow situation of analysts, the Dirks Court launched “a missile to kill a mouse” by creating a blanket personal benefit requirement.

The personal benefit requirement also protects many tippers who purposefully, knowingly, or recklessly harm others through their disclosures. For instance, the requirement appears to protect tippers who tip in order to cause harm to someone. Furthermore, even if the personal benefit requirement held liable those whose purpose is to cause harm, by treating the satisfaction of causing harm as a type of personal benefit, the requirement would still fail to hold liable those who cause the harm merely knowingly or recklessly, such as a corporate insider who becomes drunk at a bar and begins to disclose in-

170 See Dirks, 463 U.S. at 662.
171 See id. at 658–59 (discussing analysts’ useful public purpose).
172 See id. at 662; Maxwell, 341 F. Supp. 2d at 944–50 (employing the personal benefit requirement to exculpate tipper of tippee who merely used the information to trade personally).
173 341 F. Supp. 2d at 948.
174 Id. at 944–45.
175 Id. at 950.
176 Cf. Lucas v. S.C. Coastal Council, 505 U.S. 1003, 1036 (1992) (Blackmun, J., dissenting) (stating in a takings case that “today the Court launches a missile to kill a mouse” by improperly “issuing sweeping new rules to decide such a narrow case”).
178 See Yun, 327 F.3d at 1278 n.34 (stating that if a CEO’s wife disclosed information solely to humiliate her husband, she would not intend “that anyone would . . . benefit” but rather would “merely” want to harm her husband, thus implying that a personal benefit requirement would protect such a wife from tipper liability).
formation inappropriately without expecting anything in return, or the Vice President in the opening hypothetical of this Note who indifferently discusses a confidential tender offer with his barber. Unlike whistleblowers or analysts, these tippers produce no public benefit to counteract the harm they cause to investors. Thus, in protecting these tippers, the personal benefit requirement is far broader than can be justified by its motivating policy concerns.

The aforementioned flaws in the blanket personal benefit requirement suggest that although lower courts unfortunately must apply the requirement in classical cases, they should decline to extend the requirement to the misappropriation theory. Instead, courts should examine the misappropriation theory to determine what standard would best promote the text and purposes of section 10(b) of the Securities Exchange Act and Rule 10b-5 as interpreted by Supreme Court precedent, as well as the policies underlying our federal securities laws.

B. A Revised Personal Benefit Requirement for Misappropriation Cases

Instead of requiring a personal benefit in misappropriation cases, courts should require that (1) the tipper was at least reckless as to whether he or she would either benefit personally or harm the information source by tipping, and (2) the tipper was at least reckless as to whether someone in the line of tippees would use the information to trade. This standard should be subject only to the tipper’s defense that the tipper made the disclosure in a good faith attempt to prevent

---

179 See Dirks, 463 U.S. at 662 (focusing on the purpose of the disclosure in creating the personal benefit requirement); Painter et al., supra note 177, at 194 (noting that under the Dirks personal benefit test, a tipper who becomes drunk at a bar and discusses confidential information without expecting anything in return would escape section 10(b) liability); supra notes 1–3 and accompanying text.

180 See Dirks, 463 U.S. at 676–77 (Blackmun, J., dissenting) (noting that the Court created the personal benefit requirement because the “general benefit” derived from the tips outweighed the harm caused to the corporation’s shareholders); Selective Disclosure and Insider Trading, 65 Fed. Reg. 51,716, 51,716 (Aug. 24, 2000) (adopting Regulation FD and noting that trades flowing from selective disclosure cause harm to investor confidence).


182 See supra notes 158–181 and accompanying text.

183 See supra notes 158–181 and accompanying text.

184 See O'Hagan, 521 U.S. at 653, 658–59; Dirks, 463 U.S. at 652 n.8, 667 & n.27; Espionage Act, 18 U.S.C. § 794(a) (2000); Brief for Appellee, supra note 76, at 40–46; Restatement (Third) of Unfair Competition § 40 cmt. c (1995); Restatement (Second) of Agency § 395 cmt. a (1958).
criminal activity reasonably certain to cause substantial physical or financial harm to others.\textsuperscript{185} This approach not only comports with Supreme Court precedent in a technical sense, but also best promotes the important Court-identified policies of promoting investor confidence while, at the same time, protecting tippers who seek to expose criminal and harmful activity.\textsuperscript{186}

1. The Proposed Standard Expounded

First, the proposed standard establishes recklessness as the minimum mental state the tipper must possess regarding the resulting personal benefit or harm to the information source, as well as the ultimate securities trade.\textsuperscript{187} Courts should adopt the Model Penal Code’s definition of recklessness, which has become widely accepted by courts today.\textsuperscript{188} Under the Model Penal Code, a person acts recklessly if he “consciously disregards a substantial and unjustifiable risk that the material element exists or will result from his conduct.”\textsuperscript{189} Thus, under the proposed standard, the relevant inquiry would be whether the tipper consciously disregarded a substantial and unjustifiable risk that he or she would benefit personally or harm the information source, as well as a risk that he would cause a securities trade.\textsuperscript{190}

Courts should look to all relevant circumstances in determining whether these elements of the proposed standard are met.\textsuperscript{191} In the case of a personal benefit, courts should look for the types of personal benefits that Dirks suggested: pecuniary gain, reputational benefit, or benefits from making a gift to a relative or friend.\textsuperscript{192} As Dirks suggested, a tipper’s expectation that these will result could be inferred from a

\textsuperscript{185} See 18 U.S.C. § 794(a); O’Hagan, 521 U.S. at 653, 658–59; Dirks, 463 U.S. at 652 n.8, 667 & n.27; Brief for Appellee, supra note 76, at 40–46; Restatement (Third) of Unfair Competition § 40 cmt. c (1995); Restatement (Second) of Agency § 395 cmt. a (1958).

\textsuperscript{186} See O’Hagan, 521 U.S. at 653, 658–59 (emphasizing investor confidence); Dirks, 463 U.S. at 652 n.8, 667 & n.27 (emphasizing the defendant’s role in exposing fraud).

\textsuperscript{187} See supra note 184 and accompanying text.

\textsuperscript{188} See Joshua Dressler, Understanding Criminal Law § 10.07[B][3][a], at 140 (3d ed. 2001).

\textsuperscript{189} Model Penal Code § 2.02(2)(c) (1985). A risk is “substantial and unjustifiable” when “considering the nature and purpose of the actor’s conduct and the circumstances known to him, its disregard involves a gross deviation from the standard of conduct that a law-abiding person would observe in the actor’s situation.” Id.

\textsuperscript{190} Id.

\textsuperscript{191} Cf. Herman & MacLean v. Huddleston, 459 U.S. 375, 390–91 n.30 (1983) (noting that scienter in fraud cases can be inferred from circumstantial evidence).

\textsuperscript{192} See Dirks, 463 U.S. at 663–64.
relationship between the insider and the recipient that suggests a quid pro quo, or an intention to benefit the recipient of the information.\textsuperscript{193}

With regard to harming the information source, courts should consider whether there is evidence that the tipper possessed negative feelings towards the source of the information, as well as whether the information source had expressed to the tipper a strong desire for the information to remain confidential.\textsuperscript{194} Such facts would suggest that the tipper disclosed the information with some expectation that it would cause harm.\textsuperscript{195} Finally, regarding the question of whether someone in the line of tippees would trade, courts should consider whether the tipper knew about the tippee’s interest in trading in the type of stock to which the disclosure pertained, any seemingly reliable assurances made by the tippee about trading or tipping others, and the tipper’s knowledge of the trading value of the information.\textsuperscript{196}

Under the proposed standard, the tipper and tippee would not be liable, however, if the tipper made the disclosure in a good faith attempt to prevent criminal activity reasonably certain to cause substantial physical or financial harm to others.\textsuperscript{197} Thus, tippers who make disclosures to expose a corporation’s criminal fraud that is reasonably certain to cause substantial harm to investors or any other person or entity doing business with the company in the future, as the tippers in \textit{Dirks} did, would not be liable for insider trading.\textsuperscript{198} This would be true even if the disclosures were also likely to produce a personal benefit, such as an enhanced reputation, or harm the information source by exposing it to criminal liability or bankruptcy.\textsuperscript{199}

Thus, in the hypothetical in the Introduction of this Note, the Vice President-tipper and the barber-tippee would both be liable for insider trading.\textsuperscript{200} First, the Vice President consciously disregarded a substantial and unjustifiable risk that his disclosure would harm Acme

\textsuperscript{193} \textit{Id.} at 664.
\textsuperscript{194} \textit{See} \textit{Yun}, 327 F.3d at 1278 n.34 (describing a wife who discloses information to a newspaper editor in order to humiliate her husband).
\textsuperscript{195} \textit{See id.}
\textsuperscript{196} \textit{See Maxwell}, 341 F. Supp. 2d at 944 (excusing a tipper and tippee and describing facts that, under the proposed standard, would likely give rise to an inference that the insider-tipper disregarded a substantial and unjustifiable risk that the barber-tippee would trade).
\textsuperscript{197} \textit{See Dirks}, 463 U.S. at 667 (excusing the defendant-tippee and emphasizing that the tippers’ purpose was to expose corporate fraud).
\textsuperscript{198} \textit{See id.}
\textsuperscript{199} \textit{See id.} at 650 (excusing defendants despite the fact that their exposure of the corporation’s fraud caused the corrupt corporation to plummet into receivership).
\textsuperscript{200} \textit{See Model Penal Code} § 2.02(2)(c) (1985); \textit{supra} notes 1–3 and accompanying text.
Corporation, the source of the information.\textsuperscript{201} He knew that leaking information about an upcoming acquisition would create a substantial risk that the acquisition would fall apart.\textsuperscript{202} In addition, he had sufficient notice that the barber would tip his friends and that their group would collectively buy stock in Zen Corporation and even tip others, all of which would likely alert the public to the upcoming acquisition and consequently frustrate Acme Corporation’s attempt to expand its business.\textsuperscript{203} Thus, he was reckless as to whether his disclosure would harm the information source.\textsuperscript{204} For this reason, under the proposed standard it would not matter that the Vice President sought no personal benefit in making the disclosure.\textsuperscript{205}

In addition, the Vice President-tipper disregarded a substantial and unjustifiable risk that his disclosure would cause the barber-tippee to trade.\textsuperscript{206} He knew that the barber and the barber’s friends enjoyed finding and investing in acquisition targets.\textsuperscript{207} He also believed the barber was probing for information because every time he visited the barber previously, the barber had suspiciously asked whether Acme Corporation would acquire other companies soon.\textsuperscript{208} The Vice President also knew the high trading value of the information.\textsuperscript{209} Yet, the Vice President still made the disclosure.\textsuperscript{210} Thus, the Vice President was also reckless as to whether someone in the line of tippees would use the information provided by him to trade.\textsuperscript{211}

\begin{itemize}
\item \textsuperscript{201} See Model Penal Code § 2.02(2)(c) (1985); supra notes 1–3 and accompanying text.
\item \textsuperscript{202} Supra notes 1–3 and accompanying text.
\item \textsuperscript{203} See supra notes 1–3 and accompanying text.
\item \textsuperscript{204} Supra notes 1–3 and accompanying text.
\item \textsuperscript{205} See supra notes 184–199 and accompanying text. Although one might try to argue that the Vice President sought the “benefit” of speaking freely, this benefit is likely too trivial to give rise to liability. See Dirks, 463 U.S. at 663–64 (identifying personal benefits of consequence, such as a pecuniary gain, enhanced reputation, or satisfaction of making a valuable gift to a relative or friend); Maxwell, 341 F. Supp. 2d at 948 (holding that there was no personal benefit where the tipper-executive tipped his barber because “Dirks requires an intended benefit of at least some consequence” and there was no evidence that the tipper-executive sought money, a reputational gain, or the satisfaction of giving a gift to the barber); SEC v. Switzer, 590 F. Supp. 756, 766 (W.D. Okla. 1984) (holding that there was no personal benefit where a father-tipper made the disclosure for the purpose of making child care arrangements).
\item \textsuperscript{206} See Model Penal Code § 2.02(2)(c) (1985); supra notes 1–3 and accompanying text.
\item \textsuperscript{207} Supra notes 1–3 and accompanying text.
\item \textsuperscript{208} Supra notes 1–3 and accompanying text.
\item \textsuperscript{209} Supra notes 1–3 and accompanying text.
\item \textsuperscript{210} Supra notes 1–3 and accompanying text.
\item \textsuperscript{211} See Model Penal Code § 2.02(2)(c) (1985); supra notes 1–3 and accompanying text.
\end{itemize}
Moreover, the Vice President did not make the disclosure in a good faith attempt to prevent criminal activity reasonably certain to cause substantial physical or financial harm to others.\textsuperscript{212} Rather, he made his disclosure because of his indifference to the disclosure’s consequences.\textsuperscript{213} In fact, Acme Corporation was not engaged in any wrongdoing that would prompt the Vice President to disclose.\textsuperscript{214}

Finally, the barber would be liable as a trading tippee because he knew, or should have known, that the Vice President passed on information in breach of a duty to Acme Corporation.\textsuperscript{215} The barber knew that the Vice President worked for Acme Corporation and therefore, in all likelihood, was forbidden to discuss the upcoming tender offer.\textsuperscript{216}

2. Fully Protecting Investors from Trades Based on Misappropriated Information

When the U.S. Supreme Court adopted the misappropriation theory in 1997 in \textit{United States v. O’Hagan}, it made clear that the purpose of the theory is to ensure honest securities markets and thereby promote investor confidence.\textsuperscript{217} Investors will lose confidence in a market where many trades are the fruit of misuse of information.\textsuperscript{218} For that reason, the proposed standard reaches both possible misuses of information in connection with securities trades: conversion for a personal benefit, and use to the detriment of the information source.\textsuperscript{219} For the same reason, the proposed standard also holds liable tippers who cause such trades recklessly, albeit not purposefully or knowingly.\textsuperscript{220}

a. \textit{Reaching Both Types of Misuse}

An examination of other areas of law involving misuse of information reveals that improperly using information for one’s own benefit is only one type of misuse; harming the source of the informa-

\begin{footnotes}
\footnote{\textsuperscript{212} See supra notes 1–3 and accompanying text.}
\footnote{\textsuperscript{213} Supra notes 1–3 and accompanying text.}
\footnote{\textsuperscript{214} See supra notes 1–3 and accompanying text.}
\footnote{\textsuperscript{215} See United States v. Libera, 989 F.2d 596, 600 (2d Cir. 1993); SEC v. Willis, 777 F. Supp. 1165, 1169 (S.D.N.Y. 1991); supra notes 1–3 and accompanying text.}
\footnote{\textsuperscript{216} See Libera, 989 F.2d at 600; Willis, 777 F. Supp. at 1169; supra notes 1–3 and accompanying text.}
\footnote{\textsuperscript{217} \textit{O’Hagan}, 521 U.S. at 653.}
\footnote{\textsuperscript{218} Id. at 658–59.}
\footnote{\textsuperscript{219} See id.}
\footnote{\textsuperscript{220} See id.}
\end{footnotes}
tion is another.\textsuperscript{221} Perhaps the most important area of law in this regard is the law of agency because in \textit{O’Hagan} the Supreme Court itself implied that agency principles were at the misappropriation theory’s core.\textsuperscript{222} The Court not only cited to the \textit{Restatement (Second) of Agency}, but also employed standard agency language when describing the participants in misappropriation.\textsuperscript{223} For instance, the Court referred to the information source as a “principal” multiple times.\textsuperscript{224} Under these agency principles, an agent is legally obligated not to communicate information to the detriment of the principal.\textsuperscript{225} Thus, it seems that \textit{O’Hagan} strongly implied that harming the information source constitutes the type of misuse that, when connected to securities trading, the misappropriation theory ought to proscribe.\textsuperscript{226}

One need not rely solely on agency law, however, because other areas of law also demonstrate the gravity of misappropriation, through disclosure, of information to the detriment of the owner.\textsuperscript{227} For instance, under the \textit{Restatement (Third) of Unfair Competition}, one may be liable in some circumstances for disclosing a trade secret not only when disclosure is made for purposes of personal commercial exploitation, but also when disclosure is made for the purpose of causing harm to the trade secret owner.\textsuperscript{228} The same idea applies in the law of espionage; a spy violates the Espionage Act when he discloses national defense secrets with intent or reason to believe that

\textsuperscript{221} See Espionage Act, 18 U.S.C. § 794(a) (2000); Brief for Appellee, supra note 76, at 45; \textit{Restatement (Third) of Unfair Competition} § 40 cmt. c (1995); \textit{Restatement (Second) of Agency} § 395 cmt. a (1958).

\textsuperscript{222} See \textit{O’Hagan}, 521 U.S. at 652–54 (employing agency terminology and citing to the \textit{Restatement (Second) of Agency}); Brief for Appellee, supra note 76, at 42–43 (arguing that agency principles instruct the scope of the misappropriation theory); Pritchard, supra note 76, at 47 (stating that the misappropriation theory is “well grounded” in the common law of agency).

\textsuperscript{223} \textit{O’Hagan}, 521 U.S. at 652–54.

\textsuperscript{224} Id.

\textsuperscript{225} \textit{Restatement (Second) of Agency} § 395 cmt. a (1958).

\textsuperscript{226} See \textit{O’Hagan}, 521 U.S. at 652–54, 658–59; \textit{Restatement (Second) of Agency} § 395 cmt. a (1958). The SEC made this very agency argument, unsuccessfully, in \textit{Yun}. See 327 F.3d 1263, 1275 (rejecting SEC’s attempt to avoid a personal benefit requirement); Brief for Appellee, supra note 76, at 40–46 (arguing that no personal benefit should be required because, under the agency principles to which \textit{O’Hagan} alluded, a tipper breaches a duty to the information source not only when the tipper benefits from the disclosure, but also when the disclosure harms the source).


\textsuperscript{228} \textit{Restatement (Third) of Unfair Competition} § 40 cmt. c (1995).
the information will be used to the detriment of the United States. The Espionage Act does not require a personal benefit to the thief.

Together, these areas of law indicate that disclosure of information to the detriment of the information owner is equally as grave as disclosure of information for the misappropriator’s own benefit. When this misuse of information results in securities trades, the harm to investors is the same in either case; as the Supreme Court in O’Hagan made clear, investors will hesitate to invest because they will suspect that those with whom they trade may have gained their informational advantages by means the investor cannot legally match through skill or diligence.

For this reason, the Eleventh Circuit’s assertion in SEC v. Yun that O’Hagan “explicitly states or implicitly assumes” that a misappropriator must obtain a personal benefit is mistaken. Rather, O’Hagan’s emphasis on the harm caused by trades that result from misappropriation demonstrates that the Court’s occasional descriptions of a misappropriator seeking personal gain are more properly seen as reflections of the facts before the Court in which the misappropriator did trade for personal benefit.

The proposed standard’s adherence to the misappropriation theory’s underlying policy rationale justifies its modest departure from the requirements of tipper/tippee liability under the classical theory. For this reason, the Yun court’s assertion that a personal benefit requirement is proper in order to synthesize the misappropriation theory with the classical theory is also mistaken. The Yun court failed to consider that the flaws of the personal benefit requirement themselves are good reason not to impose it on the misap-

---

229 18 U.S.C. § 794(a). A person also violates the Act when he discloses the information with intent or reason to believe that it will be used to the advantage of a foreign nation. \textit{Id.}


234 See \textit{Yun}, 327 F.3d at 1275–77.
propriation theory. In addition, the Yun court displayed unwarranted concern about the possibility that failing to require a personal benefit would render Dirks a “dead letter” by inducing government prosecutors to try more cases under the misappropriation theory. It is unclear why it would be objectionable for government prosecutors to pursue a valid theory that is harmonized with law and policy merely because there happens to be an alternate theory the government cannot satisfy in that particular case. Where a defendant has violated either theory, he or she has violated Rule 10b-5, and therefore should be subject to an enforcement action. Thus, in summary, requiring either a personal benefit or harm to the information source best promotes the policies emphasized by O’Hagan.

b. Reaching Reckless Tippers

O’Hagan’s emphasis on protecting investors also suggests that tippers with a reckless state of mind should not escape liability merely because they did not hope, or know for certain, that their conduct would cause the resulting harm. This is especially true given that recklessness is no stranger to either insider trading law or other areas of criminal law; it is a common standard for liability.

Insider trading law already embraces the recklessness standard. For instance, recklessness is sufficient to establish the requisite scienter, or intent to deceive. Criminal law in general also embraces recklessness. For instance, the influential Model Penal Code states that if the legislature fails to specify what state of mind is required for

---

237 See id.
238 See id. at 1279.
239 See O’Hagan, 521 U.S. at 665 (validating the misappropriation theory as consistent with section 10(b) and Supreme Court precedent).
240 See id.
243 See Model Penal Code § 2.02(3) (1985) (setting recklessness as the default where the legislature fails to specify a mens rea, or level of intent, for an element of an offense); Quinn, supra note 51, at 891 n.147 (stating that in insider trading law, recklessness is a sufficient state of mind for scienter, or the intent to deceive).
244 See Quinn, supra note 51, at 891 n.147 (stating that in insider trading law, recklessness is a sufficient state of mind for scienter, or the intent to deceive).
245 Id.
246 See Model Penal Code § 2.02(3) (1985) (setting recklessness as the default where the legislature fails to specify a mens rea, or level of intent, for an offense).
a particular element of an offense, the default state of mind is recklessness. Applying this Model Penal Code principle to section 10(b) and Rule 10b-5 would result in a recklessness standard, since neither Congress nor the SEC specified the necessary state of mind. Thus, given O'Hagan’s emphasis on protecting investors and the general acceptance of recklessness as a minimum mental state for liability, tippers should be held liable when they recklessly cause the harmful results contained in the proposed standard.

3. Protecting Tippers Who Expose Criminal and Harmful Activity

A primary justification posited for the personal benefit requirement is that it protects tippers whose sole motive is to expose criminal and harmful activity, as was the case with the tippers in Dirks. As discussed, however, the personal benefit requirement is overly broad because it protects tippers without this commendable purpose. Thus, to protect only those tippers who commendably seek to expose criminal and harmful activity, the proposed standard allows a tipper to present the defense that he made the disclosure in a good faith attempt to prevent criminal activity reasonably certain to cause substantial physical or financial harm to others.

That this narrow defense is an appropriate balance of competing polices finds support in the analogous confidentiality exceptions of Rule 1.6 of the Model Rules of Professional Conduct. These exceptions allow a lawyer, in limited situations, to disclose confidential information about a client to prevent physical or proprietary harm. Recognizing the need to minimize the harm to client confidence that such disclosures create, the drafters of the Model Rules of Professional Conduct did not permit disclosure whenever a lawyer merely does not

---

247 Id.
250 See Dirks, 463 U.S. at 652 n.8, 667 & n.27 (emphasizing the defendant’s role in exposing fraud); id. at 676–77 (Blackmun, J., dissenting) (noting that the Court created the personal benefit requirement in the first place because the general benefit derived from the tips outweighed the harm caused to the corporation’s shareholders); Ebaugh, supra note 3, at 291–92 (arguing for a personal benefit requirement under the misappropriation theory partly in order to protect tippers who expose fraud).
251 See supra notes 170–181 and accompanying text.
252 See supra notes 170–181, 184–185 and accompanying text.
253 See Model Rules of Prof’l Conduct R. 1.6(b)(1)–(3) (2003).
254 Id.
intend to benefit personally from making it.\textsuperscript{255} Similarly, recognizing the harm to investor confidence that misuse of information through disclosure creates when that information is used to trade, the proposed standard does not permit a tipper to disclose information used for trading merely because no personal benefit is sought in making the tip.\textsuperscript{256}

4. Reconciling the Standard with the Scope of Rule 10b-5 Liability as Defined by the Supreme Court

For several reasons, the proposed standard would not threaten the established elements of Rule 10b-5 misappropriation liability. First, the tipper, as a misappropriator, would still have to engage in deception, as required by \textit{O’Hagan}.

\textsuperscript{255} See \textit{id.} at R. 1.6 cmt. 2 (emphasizing that trust is the “hallmark” of the attorney-client relationship because it encourages clients to seek legal assistance and to communicate fully).

\textsuperscript{256} See \textit{O’Hagan}, 521 U.S. at 658–59 (discussing the harm that trading on misappropriated information causes to investor confidence).

\textsuperscript{257} See \textit{id.} at 654–55.

\textsuperscript{258} See \textit{id.} at 652 (requiring a duty); \textit{Chiarella v. United States}, 445 U.S. 222, 228 (1980) (requiring a duty). The proposed standard would also leave intact the requirement that the tippee know, or should know, that the tipper breached the duty. See \textit{SEC v. Musella}, 748 F. Supp. 1028, 1038 (S.D.N.Y. 1989) (imposing the requirement).

\textsuperscript{259} See \textit{SEC v. Sargent}, 229 F.3d 68, 77 (1st Cir. 2000) (suggesting that requiring a breach of duty, without more, probably means that a personal benefit is not required); \textit{SEC v. Gonzalez de Castilla}, 184 F. Supp. 2d 365, 375 (S.D.N.Y. 2002) (treating breach of duty and personal benefit as two separate and distinct elements of tipper/tippee liability).


standard would protect those market participants who gain information through lawful skill and diligence.\textsuperscript{262}

Finally, this standard would preserve the statutory requirement that the tipper’s deception occur “in connection with” a securities trade.\textsuperscript{263} As \textit{O’Hagan} made clear, the “in connection with” requirement is satisfied when the misappropriator’s deceptive breach of duty and his or her own securities trade coincide.\textsuperscript{264} In addition, the federal securities laws tend not to distinguish between acts committed personally and acts done indirectly through other persons.\textsuperscript{265} Thus, it reasonably follows that the “in connection with” requirement may properly be satisfied where a tipper deceptively breaches a duty by recklessly causing another to trade.\textsuperscript{266}

The flexible nature of this interpretation of “in connection with” is appropriate because it serves the purposes of section 10(b).\textsuperscript{267} Although the proposed standard’s compliance with the “in connection with” requirement is more attenuated than the factual scenario addressed by \textit{O’Hagan}, in which the trading misappropriator’s deceptive breach of duty and his securities trade occurred simultaneously, the Supreme Court recently and unanimously indicated that the “in connection with” requirement may be construed flexibly, rather than technically and restrictively, in order to effectuate the purposes of section 10(b) in a reasonable manner.\textsuperscript{268} As \textit{O’Hagan} made clear, one of these purposes is to promote investor confidence, a confidence that is threatened by trades that result from informational misuse.\textsuperscript{269} Thus, the proposed standard’s heightened prevention of trades based on

\textsuperscript{262} See Pritchard, \textit{supra} note 76, at 51 (stating that requiring a breach of duty protects individuals who have gained their informational advantage through superior insight or hard work).


\textsuperscript{264} \textit{O’Hagan}, 521 U.S. at 655–56.

\textsuperscript{265} \textit{Cf. Dirks}, 463 U.S. at 659 (citing 15 U.S.C. § 78j(b)) (“[N]ot only are insiders forbidden by their fiduciary relationship from personally using undisclosed corporate information to their advantage, but they may not give such information to an outsider for the same improper purpose of exploiting the information for their personal gain.”); 17 C.F.R. § 240.14e-3(d) (2005) (providing that “it shall be unlawful . . . to communicate material, nonpublic information relating to a tender offer to any other person under circumstances in which it is reasonably foreseeable that such communication is likely to result in” trading that violates rule 14e-3).


\textsuperscript{269} \textit{O’Hagan}, 521 U.S. at 658–59.
informational misuse, through a flexible interpretation of the “in connection with” requirement, is appropriate.270

Conclusion

In misappropriation cases involving tippers and tippees, courts should not impose a requirement that the tipper intended to benefit personally from the tip. Instead, courts should require that (1) the tipper was at least reckless as to whether he or she would either benefit personally or harm the information source by tipping, and (2) the tipper was at least reckless as to whether someone in the line of tippees would use the information to trade. This standard should be subject only to the tipper’s defense that the tipper made the disclosure in a good faith attempt to prevent criminal activity reasonably certain to cause substantial physical or financial harm to others.

This standard not only comports with section 10(b), Rule 10b-5, and Supreme Court precedent, but also best promotes the important policies emphasized by the Supreme Court’s decisions: promoting investor confidence, while at the same time protecting tippers who seek to expose criminal and harmful activity. Thus, unless Congress passes a long-overdue insider trading statute, the Supreme Court should replace the personal benefit requirement with the proposed standard in tipper/tippee misappropriation cases. Lower courts, however, should not wait for Supreme Court action. While adhering to the personal benefit requirement in classical cases as they must under our system of binding precedent, lower courts should apply the proposed standard in misappropriation cases. Doing so is not only permitted, but also preferable in light of the principles and policies advanced by the Supreme Court in O’Hagan.

David T. Cohen

270 See Zanford, 535 U.S. at 819–20; O’Hagan, 521 U.S. at 658–59. By requiring the tipper to be reckless as to the resulting trade, therefore, the proposed standard also addresses the concerns raised by Yun that eliminating a personal benefit requirement might permit tipper liability absent the tipper having “even the slightest” intent for someone else to trade. See 327 F.3d at 1278.
TERRORIZING JUSTICE: AN ARGUMENT THAT PLEA BARGAINS STRUCK UNDER THE THREAT OF “ENEMY COMBATANT” DETENTION VIOLATE THE RIGHT TO DUE PROCESS

Abstract: As part of the War on Terror, the President has detained certain individuals as “enemy combatants”—a form of military detention that is preventive, non-criminal, and of indefinite duration. Some terrorism defendants appear to have pled guilty to criminal charges in order to avoid being detained as enemy combatants. This Note argues that plea bargains induced by threats of enemy combatant detention do not arise from the normal give-and-take of plea bargaining, create serious public policy concerns, and serve no societal interests that could not be served equally well by other means. It therefore concludes that the courts should hold such plea bargains per se unenforceable under the Due Process Clause of the Fifth Amendment.

Introduction

He took a cigarette out of the case and forced it into Rubashov’s mouth without letting go his coat button. ‘You’re behaving like an infant. Like a romantic infant,’ he added. ‘Now we are going to concoct a nice little confession and that will be all for today.’

… ‘It is not in my interest to lay you open to mental shocks. All that only drives you further into your moral exaltation. I need you sober and logical. My only interest is that you should calmly think your case to a conclusion. For, when you have thought the whole thing to a conclusion—then, and only then, will you capitulate.’

—Arthur Koestler

In Arthur Koestler’s Cold War-era novel Darkness at Noon, set during the Soviet show trials of the 1930s, the interrogator poses a choice to the protagonist Rubashov: either insist on his innocence and be summarily sentenced to death in a secret administrative trial, or con-

---

fess at a public trial and gain the interrogator’s assistance in reducing his sentence.2

Since the Al Qaeda terrorist attacks of September 11, 2001, U.S. President George W. Bush has claimed the authority to designate individuals as “enemy combatants” and detain them under military authority indefinitely, without charges and without a criminal trial.3 Enemy combatant detention is a form of preventive military detention that carries minimal due process guarantees (for example, the government need not accuse the detainee of any particular wrongful acts, and the detainee bears the burden of disproving the government’s factual allegations in any challenge to the detention).4 It also involves confinement in unusually restrictive conditions for an uncertain, potentially lifelong, duration.5 Many commentators have argued that

---

2 Id. at 106.
3 Brief for the Respondents at 25–27, Hamdi v. Rumsfeld, 542 U.S. 507 (2004) (No. 03-6696); see Brief for the Petitioners at 38, Rumsfeld v. Padilla (Padilla I), 542 U.S. 426 (2004) (No. 03-1027). No all-encompassing definition for the term “enemy combatant” exists because the government has provided only specific examples of people who could be designated enemy combatants, without providing any examples of people who could not be designated enemy combatants. See In re Guantanamo Detainee Cases, 355 F. Supp. 2d 443, 475 (D.D.C. 2005). In Hamdi v. Rumsfeld, the Supreme Court established that the term encompasses any person, whether a U.S. citizen or a foreign national, who engages in foreign armed conflict against the United States or directly assists enemy forces engaging in such hostilities. See 542 U.S. at 516–17; see also Guantanamo Detainee Cases, 355 F. Supp. 2d at 475. The government also asserts that the term may encompass some individuals who have neither committed any belligerent act against U.S. forces nor directly assisted such acts, such as a little old lady who writes checks to what she believes is a charity but is actually an Al Qaeda front, an English teacher who provides language instruction to the son of an Al Qaeda member, and a journalist who refuses to disclose the location of Osama bin Laden. Guantánamo Detainee Cases, 355 F. Supp. 2d at 475. In addition, the government asserts that the locus of capture is irrelevant; a person may be designated an enemy combatant regardless of whether that person is on U.S. soil or abroad. See Brief for the Petitioners, supra, at 30; see also Padilla v. Hanft (Padilla II), 423 F.3d 386, 392 (4th Cir. 2005), cert. denied, No. 05-533, 2006 WL 845383 (U.S. Apr. 3, 2006). The Supreme Court has twice declined to rule on the question of whether a U.S. citizen captured in the United States may be designated an enemy combatant, and has not yet been confronted with a case in which a foreign national captured in the United States may be designated an enemy combatant. See Padilla v. Hanft (Padilla V), No. 05-533, 2006 WL 845383, at *2 (U.S. Apr. 3, 2006) (denying certiorari); Padilla I, 542 U.S. at 430 (reversing the court on jurisdictional grounds); see also Al-Marri v. Hanft, 378 F. Supp. 2d 673 (D.S.C. 2005) (holding as proper the detention as an enemy combatant of a foreign national captured in the United States).
4 See Hamdi, 542 U.S. at 533–34, 538 (describing the limited due process guarantees for enemy combatants).
5 See Guantánamo Detainee Cases, 355 F. Supp. 2d at 465 (noting that because the government has conceded that the War on Terror could last for several generations, enemy combatant detention may well amount to a life sentence); David Cole, Enemy Aliens: Double Standards and Constitutional Freedoms in the War on Terrorism 41
this asserted power to designate individuals as enemy combatants violates the individuals’ due process rights, undermines fundamental principles of democratic governance, and borrows from the worst traditions of wartime repression in America and abroad. Justice Stevens opined, in dissent to one pro-government enemy combatant decision, that this kind of executive branch detention is “the hallmark of the Star Chamber.” Nevertheless, few scholarly articles have addressed the harms caused by allowing the military, preventive-detention imperatives of enemy combatant detention to contaminate the criminal justice system.


7 Padilla I, 542 U.S. at 465 (Stevens, J., dissenting) (rejecting the Court’s holding that the enemy combatant’s challenge to his detention should be dismissed on jurisdictional grounds). The Court of Star Chamber was a special court convened by the King of England that was known for its secrecy and disregard for individual rights, and its name is often invoked as a symbol of abuse of power. See, e.g., Faretta v. California, 422 U.S. 806, 821 (1975) (describing the Star Chamber as a centuries-old symbol of disregard for basic rights); Green v. United States, 356 U.S. 165, 202–03 (1958) (Black, J., dissenting) (describing the Star Chamber as an “odious instrument of tyranny” whose arbitrary procedures and gross excesses inspired many of the safeguards included in the U.S. Constitution); Ullmann v. United States, 350 U.S. 422, 428 (1956) (describing the Fifth Amendment privilege against self-incrimination as being aimed at preventing a recurrence of the abuses of the Spanish Inquisition and the Star Chamber); In re Oliver, 333 U.S. 257, 268–70 (1948) (describing the Star Chamber as a symbol of menace to liberty that is in part responsible for the Anglo-American distrust for secret trials).

8 See Lee Epstein et al., The Supreme Court During Crisis: How War Affects Only Non-War Cases, 80 N.Y.U. L. REV. 1, 94–111 (2005) (arguing that in times of war, including the War on Terror, wartime conditions affect the Supreme Court’s disposition of ordinary civil rights and civil liberties cases more than they affect the disposition of cases directly related to war); Peter Margulies, Judging Terror in the “Zone of Twilight”: Exigency, Institutional Equity, and Procedure After September 11, 84 B.U. L. REV. 383, 431–36 (2004) (criticizing the compromise that the district court struck in United States v. Moussaoui, 282 F. Supp. 2d 480 (E.D. Va. 2003) between the defendant’s interest in gaining access to an Al Qaeda witness in U.S. custody, and the national security interest in denying such access); Radack, supra note 6, at 541–42 (arguing that the “revolving door” between military detention and civilian prosecutions undermines the legitimacy of both systems); Andrew T. Jackola, Comment, A Second Bite at the Apple. How the Government’s Use of the Doctrine of Enemy Combatants in the Case of Zacarias Moussaoui Threatens to Upset the Future of the Criminal Justice System, 27 HAMLINE L. REV. 101, 125–31 (2004) (arguing that the possibility that a terrorism defendant could be tried for the same offense by both the criminal justice system and a military tribunal implicates double jeopardy concerns).

Although some scholars have mentioned the potential influence of enemy combatant threats on plea bargaining, they have not analyzed it in great detail. See Susan M. Akram & Maritza Karmely, Immigration and Constitutional Consequences of Post-9/11 Policies Involving
When a prosecutor uses the threat of enemy combatant detention as leverage in a criminal case, the threat creates extraordinary pressure to plead guilty, not unlike the pressure on Rubashov to capitulate.\textsuperscript{9} A pair of terrorism prosecutions illustrates how this pressure operates.\textsuperscript{10} In March 2003, the Federal Bureau of Investigation (the
approached Iyman Faris, a naturalized U.S. citizen from Kashmir, to investigate his possible links to terrorist organizations. After Faris agreed to cooperate, the agents took him to Quantico, Virginia, where, according to the attorney representing Faris on appeal, the FBI kept Faris under guard and subjected him to almost daily interrogations. After more than two weeks, Faris met for the first time with his court-appointed defense counsel. According to press accounts and Faris’s attorney, the FBI put intense pressure on Faris to plead guilty to providing material support to terrorism; within four days of being appointed, Faris’s attorney advised him that if he did not plead guilty, the Defense Department would designate him an enemy combatant and ship him to Guantanamo Bay. Faris chose to accept the plea bargain and was sentenced to twenty years in prison.

During the same year, Qatari citizen Ali Saleh Kahlah al-Marri was under indictment for terrorism-related financial fraud and lying to the FBI about his phone calls to the Middle East. Al-Marri intended to proceed to trial, but one month before the scheduled trial date, President Bush declared him an enemy combatant. The gov-
The government still holds al-Marri as an enemy combatant.\textsuperscript{18} The two cases, resolved within days of each other, sent a clear message to terrorism defendants: either plead guilty and accept a fixed sentence from the Justice Department, or refuse to cooperate and be thrown into the legal black hole of enemy combatant detention.\textsuperscript{19}

This Note argues that in the context of the War on Terror, the threat of extrajudicial enemy combatant detention—an indefinite, preventive, and non-criminal military detention—puts unique and intolerable pressure on the plea bargaining process.\textsuperscript{20} Forcing defendants to choose between enemy combatant detention and a guilty plea is far more coercive than making them choose between a trial, with its attendant risk of a conviction on more serious charges, and a guilty plea.\textsuperscript{21} In addition, plea bargains induced by threats of enemy combatant detention (hereinafter “enemy combatant threat bargains”) let military imperatives, rather than criminal justice imperatives, drive the plea bargaining process.\textsuperscript{22} Enforcing such bargains corrodes both the integrity of the criminal justice system and the rule of law.\textsuperscript{23} This Note therefore concludes that the courts should hold enemy combatant threat bargains per se unenforceable under the Due Process Clause of the Fifth Amendment.\textsuperscript{24}

\textsuperscript{18} See Al-Marri, 378 F. Supp. 2d at 680–82 (denying al-Marri’s motion for summary judgment on his petition for a writ of habeas corpus).

\textsuperscript{19} See Eric Lichtblau, \textit{Wide Impact from Enemy Combatant Detention Is Seen}, \textit{N.Y. Times}, June 25, 2003, at A14 (reporting that “a senior F.B.I. official said today that the Marri decision held clear implications for other terrorism suspects. ‘If I were in their shoes, I’d take a message from this,’ the official said”).

\textsuperscript{20} See infra notes 183–282 and accompanying text.

\textsuperscript{21} See infra notes 183–282 and accompanying text.

\textsuperscript{22} See infra notes 246–255 and accompanying text. The term “enemy combatant threat bargains” is the author’s own.

\textsuperscript{23} See infra notes 246–255 and accompanying text.

\textsuperscript{24} See infra notes 256–282 and accompanying text. Terrorism prosecutions are almost always a matter of federal criminal enforcement, and enemy combatant detention is itself an exercise of federal power. See \textit{Hamdi}, 542 U.S. at 517–18 (describing the President’s power to detain enemy combatants as being incident to waging war); Attorney General Alberto R. Gonzalez, Remarks to Department of Justice Employees (Feb. 4, 2005), (transcript available at http://www.justice.gov/opa/pr/2005/February/05_ag_045.htm) (stating, upon his confirmation as Attorney General, that protecting the United States from terrorism is the Justice Department’s “top priority”). For that reason, this Note focuses on the Due Process Clause of the Fifth Amendment, which curtails federal power, and not on the Fourteenth Amendment, which curtails the power of the states. See U.S. Const. amend. XIV; U.S. Const. amend. V.
Part I of this Note introduces the role of plea bargains in the U.S. criminal justice system and examines the standards for the enforceability of plea bargains in traditional criminal justice contexts. It also describes the related category of release-dismissal agreements, which courts have been more hesitant to enforce. Part II describes the enemy combatant detention power and its relevance to criminal prosecutions in the War on Terror. Part III contends that enemy combatant threat bargains do not arise from the normal give-and-take of plea bargaining, create serious public policy concerns, and serve no societal interests that could not be served equally well by other means. It therefore concludes that the courts should hold enemy combatant threat bargains per se unenforceable under the Due Process Clause.

I. The Enforceability of Plea Bargains in Traditional Criminal Contexts

A. Plea Bargains Generally

Plea bargaining is the process by which a prosecutor and a criminal defendant negotiate an agreement, where the defendant pleads guilty to a lesser offense or to a particular charge in exchange for some concession by the prosecutor, such as a more lenient sentence or a dismissal of other charges. In 1971, in *Santobello v. New York*, the U.S. Supreme Court succinctly summarized why plea bargaining is an essential feature of the U.S. criminal justice system: it leads to prompt and largely final disposition of most criminal cases, it avoids much of the corrosive impact of a defendant’s enforced idleness during pretrial confinement, it protects the public from the chance that a defendant would commit new crimes while on pretrial release, and, by

---

25 *See infra* notes 30–86 and accompanying text.
26 *See infra* notes 87–108 and accompanying text.
27 *See infra* notes 109–182 and accompanying text.
28 *See infra* notes 183–255 and accompanying text.
29 *See infra* notes 256–282 and accompanying text.
shortening the time between charge and disposition, it enhances the rehabilitative prospects of guilty defendants.\textsuperscript{31}

Without the prompt disposition of cases through plea bargaining, unresolved cases would flood the criminal justice system.\textsuperscript{32} In 2003, for example, only 4\% of the 85,106 federal criminal defendants exercised their right to a trial, and guilty pleas constituted nearly 96\% of the 75,805 convictions that year.\textsuperscript{33} Yet as indispensable as plea bargaining is to the judicial system, it also carries significant potential for abuse.\textsuperscript{34} By pleading guilty to a crime, the defendant relieves the prosecution of the burden of proving its case, and waives his or her privilege against self-incrimination, right to trial by jury, right to confront his or her accusers, and most evidentiary objections.\textsuperscript{35} In 1968, in \textit{Boykin v. Alabama}, the Supreme Court pointedly recognized this potential for abuse, observing that a plea bargain obtained by means of prosecutorial coercion or threats, or through the defendant’s ignorance, fear, or lack of comprehension, can serve as “a perfect cover-up of unconstitutionality.”\textsuperscript{36} In an effort to guard against such abuses

\begin{itemize}
\item \textsuperscript{31}404 U.S. 257, 260–61 (1971) (holding that prosecutors must keep the promises they make to defendants in plea bargains).
\item \textsuperscript{32}Id. at 260 (noting that if every criminal charge resulted in a jury trial, federal and state governments would have a great need for more judges and court facilities).
\item \textsuperscript{34} See John W. Keker, \textit{The Advent of the ‘Vanishing Trial’: Why Trials Matter}, Champion, Sept.–Oct. 2005, at 32–35 (arguing that the widespread use of plea bargains interferes with public scrutiny of the judicial system and deprives the defense bar of any way of keeping overzealous prosecutors in check).
\item \textsuperscript{35}Boykin v. Alabama, 395 U.S. 238, 242–43 (1969) (reversing the conviction of a criminal defendant because the record did not clearly establish that his guilty plea was knowing and voluntary); see McMann v. Richardson, 397 U.S. 759, 770–71 (1970) (holding that, where a defendant pled guilty based on counsel’s incorrect conclusion that a prior coerced confession would be admissible at trial, the defendant assumed the risk that his attorney was mistaken on either the facts or the law, as long as the attorney was reasonably competent and made those mistakes in good faith).
\item \textsuperscript{36}395 U.S. at 243. Indeed, although the Supreme Court seldom finds unequal bargaining power in plea negotiations, many scholars and lower courts have expressed concerns about the relative bargaining power of the prosecutor and the defendant. Compare Bordenkircher v. Hayes, 434 U.S. 357, 362 (1978) (describing the “give-and-take” of plea negotiation as a situation in which the prosecutor and the defendant possess relatively equal bargaining power) (quoting Parker v. North Carolina, 397 U.S. 790, 809 (1969) (Brennan, J., dissenting)), with United States v. Mezzanatto, 513 U.S. 196, 216 (1995) (Souter, J., dissenting) (noting that defendants are generally in no position to challenge the standard form waivers that many prosecutors require as a condition of entering into plea negotiations), United States v. Green, 346 F. Supp. 2d 259, 265–76 (D. Mass. 2004) (observing that various structural elements of plea bargaining, and sentencing guidelines in particular, place enormous power in the hands of federal prosecutors and give rise to a
while preserving the finality of most plea bargains, the Supreme Court requires any guilty plea to be made voluntarily and intelligently. Yet the question remains: what kinds of coercion or unequal bargaining power can render a plea involuntary?

B. Statutory Structures That Improperly Encourage Guilty Pleas and Their Effect on Voluntariness

When a criminal statute mandates a lesser punishment for those who plead guilty but allows a heavier punishment for those found guilty at trial, the imposition of the heavy punishment may be unconstitutional. In 1967, in United States v. Jackson, the Supreme Court held unenforceable the death penalty clause of the Federal Kidnapping Act, a criminal statute, because the statute exposed the defendant to a possible death sentence after a jury trial but only to a potential life sentence after a guilty plea. After being indicted under this statute, Jackson and his co-defendants moved to dismiss the indictment, arguing that the death-by-jury, life-by-plea structure of the statute impermissibly burdened their Sixth Amendment rights to a jury trial and their Fifth Amendment due process rights. In response, the government asserted that because this structure served Congress’s interest in avoiding the harshness of a mandatory death penalty for all capital convictions, the statute’s incidental effect on the defendants’ decision making was unimportant. The Supreme Court rejected the
government’s argument.\textsuperscript{43} Because the statute’s inevitable effect was to penalize defendants for exercising their Sixth Amendment right to a jury trial, and this effect was not necessary in order to carry out the government’s goal of imposing a non-mandatory death penalty, the Court reasoned that the statute impermissibly burdened the defendants’ exercise of their constitutional rights.\textsuperscript{44} The Court therefore held the death penalty clause of the statute unenforceable.\textsuperscript{45}

In subsequent cases, however, the Supreme Court declined to incorporate \textit{Jackson} principles into its analyses of the voluntariness of plea bargains, and applied \textit{Jackson} only in cases involving jury verdicts.\textsuperscript{46} As a result of these later decisions, a guilty plea is much less vulnerable to attack under \textit{Jackson} than a jury’s guilty verdict.\textsuperscript{47}

In 1970, in \textit{Brady v. United States}, the first of the post-\textit{Jackson} plea bargaining cases, the Court refused to grant relief to a defendant who pled guilty under the Federal Kidnapping Act, the same statute whose death penalty clause the Court held unconstitutional in \textit{Jackson}.\textsuperscript{48} Brady initially pled not guilty, but he changed his plea to guilty after he learned that his co-defendant had confessed and was planning to testify against him.\textsuperscript{49} After being sentenced to fifty years in prison, Brady attacked the voluntariness of his plea, arguing that because fear of death was a factor in his decision to plead guilty, the plea should be invalidated.\textsuperscript{50} The Supreme Court held that, even if Brady would not have pled guilty but for the unconstitutional death penalty provision, the plea was not necessarily involuntary.\textsuperscript{51} In this situation, the Court held, Brady’s plea would have been involuntary only if the fear of

\textsuperscript{43} Id. at 582–83.
\textsuperscript{44} Jackson, 390 U.S. at 582–83.
\textsuperscript{45} Id. at 591. In reaching this remedy, the Court considered and rejected a number of other possible remedies. \textit{Id.} at 583–85. The Court reasoned that merely rejecting coerced pleas would alleviate but not completely eliminate the constitutional infirmity, because not every defendant who pled guilty to violating the statute necessarily did so involuntarily. \textit{Id.} at 583. The Court also refused to issue a rule precluding all defendants from pleading guilty under the statute, because this would rob the criminal process of too much flexibility and modify the operation of the statute in a manner more appropriate for Congress to undertake. \textit{Id.} at 585. Finally, the Court refused to strike down the entire statute, reasoning that the death penalty clause was severable from the remainder of the statute. \textit{Id.} at 585–86.
\textsuperscript{46} See infra notes 48–65 and accompanying text.
\textsuperscript{47} See infra notes 48–65 and accompanying text.
\textsuperscript{49} Id. at 743. Brady entered his plea prior to the Court’s decision in \textit{Jackson}. See \textit{id.}
\textsuperscript{50} Id. at 744, 746. Specifically, Brady filed a habeas corpus petition under 28 U.S.C. § 2255. \textit{Id.} at 744.
\textsuperscript{51} Id. at 750.
death or hope of leniency gripped him so tightly that, with the assistance of counsel, he did not or could not choose rationally between risking a trial or pleading guilty.\textsuperscript{52} The Court embraced this broad voluntariness standard because it could not distinguish Brady’s predicament from that of any other defendant who feared receiving a greater penalty at trial.\textsuperscript{53} And if a defendant’s fear of receiving a greater penalty at trial could, without more, invalidate a guilty plea, then no plea bargain could survive attack.\textsuperscript{54} Such a result would be against public policy, the Court reasoned, because it would eliminate the mutual benefits that plea bargaining creates for the state and the defendant: the state saves scarce judicial resources and obtains prompt punishment, and the defendant limits his exposure and avoids the burdens of a trial.\textsuperscript{55} Thus, the Court held that Brady voluntarily entered his guilty plea.\textsuperscript{56} Other decisions, including two decided on the same day as \textit{Brady}, made clear that \textit{Brady}’s voluntariness standard applied to all plea bargains struck under similar death-by-jury, life-by-plea statutes.\textsuperscript{57}

\textsuperscript{52} \textit{Id.} The Court in \textit{Brady} drew a sharp distinction between defendants pleading guilty without the assistance of counsel and defendants pleading guilty while represented by counsel. \textit{See id.} at 753–55. Pleas without counsel, however, are beyond the scope of this Note because indigent persons charged with criminal offenses have the right to an appointed attorney. \textit{See Gideon v. Wainwright}, 372 U.S. 335, 342–45 (1963) (holding that legal counsel must be made available to criminal defendants who cannot retain counsel). Although one heavily publicized terrorism defendant chose to proceed pro se and then unexpectedly chose to plead guilty, the author is not aware of any terrorism defendants who engaged in plea bargaining without the assistance of counsel. \textit{See United States v. Moussaoui}, No. 01CR455 (E.D. Va. Apr. 25, 2005) (order denying a sealed motion by defendant Zacarias Moussaoui’s court-appointed counsel to rescind Moussaoui’s unrepresented guilty plea); Motion by Zacarias Moussaoui to Dismiss Court-Appointed Counsel and Proceed Pro Se, \textit{Moussaoui}, No. 01CR455 (stating, in a motion handwritten by the defendant in his prison cell, that the defendant rejects the “imposition” of his court-appointed lawyers and wishes to proceed pro se).

\textsuperscript{53} \textit{Brady}, 397 U.S. at 751–52. In a related decision, Justice Brennan criticized the \textit{Brady} standard as apparently requiring the defendant’s mental state to border on temporary insanity to render the guilty plea involuntary. \textit{Parker v. North Carolina}, 397 U.S. 790, 800 n.2 (1970) (Brennan, J., dissenting).

\textsuperscript{54} \textit{Brady}, 397 U.S. at 753.

\textsuperscript{55} \textit{Id.} at 752–53.

\textsuperscript{56} \textit{Id.} at 756–77.

\textsuperscript{57} \textit{See Parker}, 397 U.S. at 798; \textit{Richardson}, 397 U.S. at 771. In \textit{Parker v. North Carolina}, the Court refused to grant relief to a defendant who pled guilty based on a combination of incorrect legal advice and death-by-jury, life-by-plea pressures. \textit{Parker}, 397 U.S. at 797–98. Parker argued that the Court should hold his plea involuntary because he was convicted under a statutory framework essentially identical to that held unconstitutional in \textit{Jackson}. \textit{Id.} at 794. Justice Brennan, joined by Justices Douglas and Marshall, dissented from the Court’s rejection of this argument, contending that the majority’s decision undermined the rationale of \textit{Jackson} by making it essentially impossible for defendants to rescind a
In 1978, in *Corbitt v. New Jersey*, the Court limited the reach of *Jackson* in non-capital cases, refusing to extend *Jackson* principles to a statute that involved a potential life sentence rather than the death penalty and that allowed, but did not mandate, a lighter sentence for guilty pleas. 58 New Jersey prosecutors charged defendant Corbitt with first-degree murder under a New Jersey statute that imposed mandatory life imprisonment for first-degree murder jury convictions, but gave judges discretion over the penalty for those pleading nolo contendere. 59 Corbitt pled not guilty, the jury convicted him at trial, and he received the mandatory sentence of life imprisonment, which he subsequently challenged. 60 The Court distinguished *Jackson* because the pressures on Corbitt to forgo trial did not rise to the same magnitude as the pressures in *Jackson*. 61 First, Corbitt did not face the unique severity and irrevocability of the death penalty. 62 Second, because life imprisonment remained within the judge’s sentencing discretion after accepting Corbitt’s plea, pleading nolo contendere did not reduce Corbitt’s sentencing exposure. 63 Unconvinced that the New Jersey statute exerted unconstitutionally powerful coercion for innocent defendants to plead nolo contendere, the Court affirmed Corbitt’s sentence. 64 Thus, by the late 1970s, the Court had defined “voluntariness” in a way that made it very difficult for defendants to invalidate plea bargains even when *Jackson* principles applied, and it had limited *Jackson* principles to situations in which a guilty plea based on unconstitutional coercion. Id. at 799–800 (Brennan, J., dissenting). Justice Brennan argued that plea bargains obtained through unconstitutional pressures give rise to a clear danger that innocent people would plead guilty, and so should be subjected to greater scrutiny than other plea bargains. See id. at 807–10 (Brennan, J., dissenting). Also on the same day, in *McMann v. Richardson*, the Court explicitly held that a defendant cannot overturn an otherwise valid guilty plea by proof that the plea was motivated by a prior coerced confession. 397 U.S. at 771. Justice Brennan, joined by Justices Douglas and Marshall, dissented, arguing that the majority elevated form over substance in what he characterized as a rankly unfair effort to preserve the sanctity of virtually all plea bargains. Id. at 786 (Brennan, J., dissenting). In 1971, in *Atkinson v. North Carolina*, the Court reaffirmed that *Jackson* was still good law—that its recent decisions had limited rather than overruled it. *Atkinson v. North Carolina*, 403 U.S. 948, 948 (1971) (mem.). Without any opinion beyond a citation to *Jackson*, the Court reversed a death sentence imposed by North Carolina’s death-by-jury, life-by-plea capital statute. Id. at 948 (citing generally *Jackson*, 390 U.S. 570).

---

59 Id. at 215–16.
60 Corbitt, 439 U.S. at 216.
61 Id. at 217; see also *Jackson*, 397 U.S. at 583.
62 Id. at 217.
63 Id. at 217.
64 Id. at 225.
essarily prevented the court from imposing an unusually severe maximum punishment.  

C. Proper and Improper Prosecutorial Threats in Plea Bargaining

The Court’s reasoning in *Jackson* opened the door for defendants to argue that prosecutorial threats to punish defendants more harshly for exercising their right to a jury trial would, like the statutory structure at issue in *Jackson*, be constitutionally suspect because such threats exert improper pressure on the defendant to plead guilty.  

In *Jackson*, the Court stated in dicta that if the statutory scheme had served no other purpose than to chill the assertion of constitutional rights by penalizing those who exercise them, then it would clearly violate the defendant’s right to due process. This raised the question of whether a *prosecutorial strategy* that chilled defendants’ assertion of their right to a jury trial by penalizing those who exercised that right would be similarly unconstitutional.

Over the next eight years, the Supreme Court reserved that specific question but struck down efforts of judges and prosecutors to chill the right of defendants to appeal. In 1969, in *North Carolina v. Pearce*, the Supreme Court held unconstitutional a trial court’s punishment of defendants for appealing their original convictions by imposing heavier sentences on retrial. Drawing an analogy to *Jackson*, the Court held that such vindictive resentencing is unconstitutional because it chills the exercise of a basic due process right—the right to appeal. In 1974, in *Blackledge v. Perry*, the Court extended *Pearce* to prosecutorial strategies that chilled the defendant’s right to appeal. After the *Perry* defendant appealed a misdemeanor conviction, the prosecutor reindicted him for the same conduct, but this time

---

65 See id. at 217; *Parker*, 397 U.S. at 795; *Richardson*, 397 U.S. at 771; *Brady*, 397 U.S. at 750.
66 See *Jackson*, 397 U.S. at 583.
67 Id. at 581.
68 See id.
69 See Blackledge v. Perry, 417 U.S. 21, 28–29 (1974); *Brady*, 397 U.S. at 751 n.8; *North Carolina v. Pearce*, 395 U.S. 711, 723 (1969). In 1970, in *Brady*, the Court reserved the question, expressly stating that its holding (refusing to find coercion where the defendant pled guilty out of fear of the death penalty) did not cover situations in which the prosecutor or the judge “deliberately employ[ed] their charging and sentencing powers to induce a particular defendant to tender a plea of guilty.” 397 U.S. at 751 n.8.
70 395 U.S. at 723.
71 Id. at 724.
72 417 U.S. at 25.
charged the defendant with a felony.\textsuperscript{73} The defendant pled guilty to the new indictment and then filed a habeas corpus petition arguing that the felony indictment deprived him of due process of law.\textsuperscript{74} The Court declined to enforce the guilty plea because the new indictment unconstitutionally created a fear of prosecutorial vindictiveness.\textsuperscript{75} Significantly, the Court held that the defendant did not have to establish that the prosecutor actually had a retaliatory motive; what mattered was that the increase from a misdemeanor to a felony indictment gave rise to a fear of vindictiveness, chilling all but the hardiest of defendants from exercising their right to appeal.\textsuperscript{76}

In 1977, however, in \textit{Bordenkircher v. Hayes}, the Court held that a prosecutor’s threat during plea negotiations to indict the defendant on a more serious charge if he refused to plead guilty was a permissible bargaining tactic.\textsuperscript{77} In \textit{Hayes}, the prosecutor first indicted Hayes on a charge punishable by two to ten years in prison.\textsuperscript{78} During plea negotiations, the prosecutor offered Hayes a sentence of five years if he pled guilty, but warned Hayes that if he did not plead guilty, the prosecutor would seek a superseding indictment under a different statute—one that would subject Hayes, if convicted, to mandatory life imprisonment.\textsuperscript{79} Hayes refused the offer, and the prosecutor indicted him under the life imprisonment statute.\textsuperscript{80} In addressing Hayes’s claim of a violation of due process, the Court distinguished \textit{Pearce} and

\textsuperscript{73} \textit{Id.} at 23. At the time, North Carolina law provided for two different tiers of trial courts, the District Court and the Superior Court. \textit{Id.} at 22. The District Court had exclusive jurisdiction for the trial of misdemeanors, but a person convicted in the District Court decisions had the right to a trial de novo in the Superior Court. \textit{Id.} If the defendant took such an appeal, then the prior conviction would be annulled and the prosecution would begin with a clean slate in the Superior Court. \textit{Id.} Here, Perry was convicted of a misdemeanor in the District Court and filed a notice of appeal for trial de novo in the Superior Court. \textit{Id.} at 23. After the notice of appeal but before the new trial, the prosecutor indicted Perry for a felony arising from the same conduct for which Perry had been tried in the District Court. \textit{Id.}

\textsuperscript{74} \textit{Id.} at 21. The defendant also raised a double jeopardy claim, but the Court did not address this because his due process claim was dispositive. \textit{Id.} at 25.

\textsuperscript{75} \textit{Id.} at 27–28.

\textsuperscript{76} \textit{Id.} at 28.

\textsuperscript{77} 434 U.S. at 365.

\textsuperscript{78} \textit{Id.} at 358.

\textsuperscript{79} \textit{Id.} at 358–59. As Justice Powell noted in dissent, the prosecutor’s offer of a five-year sentence was hardly generous for the original offense charged—uttering one forged check in the amount of $88.30. \textit{Id.} at 369 (Powell, J., dissenting).

\textsuperscript{80} \textit{Id.} at 359. Both parties stipulated that the prosecutor possessed sufficient evidence to support the superseding indictment at the time of his threat, and that the prosecutor sought the superseding indictment only because of Hayes’s refusal to plead guilty to the original charge. \textit{Id.}
Perry because those cases dealt with state retaliation against defendants who chose to appeal their convictions, rather than state pressure to plead guilty during the “normal give-and-take negotiation” of plea bargaining. In the give-and-take of plea bargaining, the Court held, a prosecutor’s threats of new or heavier charges carry no element of improper punishment or retaliation as long as the defendant is free to accept or reject the prosecution’s offer. The prosecutor has a legitimate interest at the bargaining table to persuade the defendant to waive his right to a trial and has broad discretion to decide what charges to file. The fact that the prosecutor openly presented the defendant with a choice between forgoing trial or facing legitimate but more serious charges at trial did not violate the Due Process Clause of the Fourteenth Amendment. Thus, under Pearce and Perry, a plea bargain may be unenforceable if it chills the exercise of a fundamental right, such as the right to appeal errors of fact or law. But under Hayes, threats that form part of the normal give-and-take of plea bargaining, such as threats to file new criminal charges, are permissible—even though they tend to chill the defendant from exercising the right to a jury trial.

D. Judicial Hesitation to Enforce Release-Dismissal Agreements

Hayes suggests that prosecutorial threats regarding the criminal justice consequences of refusing a plea bargain are almost always a permissible part of the normal give-and-take of plea bargaining. But as the example of release-dismissal agreements illustrates, threats unrelated to criminal justice objectives are not part of the normal give-and-take of plea bargaining. A release-dismissal agreement is an arrangement whereby a prosecutor agrees to dismiss pending criminal

81 Id. at 362–63.
82 Hayes, 434 U.S. at 363.
83 Id. at 364–65.
84 Id.
85 See Perry, 417 U.S. at 28–29; Pearce, 395 U.S. at 723.
87 See id.; Parker, 397 U.S. at 800 & n.2 (Brennan, J., dissenting) (describing the majority’s opinion as never allowing the unconstitutional pressure identified in Jackson to vitiate a guilty plea except in highly unrealistic hypothetical situations, and opining that the majority apparently requires the defendant’s mental state to border on temporary insanity for his or her guilty plea to be involuntary).
charges against a person, in exchange for that person agreeing not to sue public officials for alleged deprivations of constitutional rights.  

Although release-dismissal agreements appear superficially similar to normal, purely criminal plea bargains, a different standard governs their enforceability. For many years, courts viewed release-dismissal agreements with great suspicion, sometimes holding all such agreements void as against public policy. In 1968, for example, in Dixon v. District of Columbia, the U.S. Court of Appeals for the D.C. Circuit expressed concerns that release-dismissal agreements suppress legitimate complaints against police misconduct and tempt prosecutors to trump up charges; the court not only refused to enforce any release-dismissal agreements, but it also barred prosecutors from filing new charges against a defendant after he breached such an agreement. In 1970, in MacDonald v. Musick, the U.S. Court of Appeals for the Ninth Circuit went further, characterizing a prosecutor’s decision to seek a release-dismissal agreement as a form of extortion that also violated state attorney ethics rules. 

In 1987, in Town of Newton v. Rumery, the Supreme Court set to rest some of the ethical and enforceability questions surrounding release-dismissal agreements. The Court held, by a 5-to-4 margin, both that a

89 See id. at 389–94.
90 See id.
91 See Rumery v. Town of Newton, 778 F.2d 66, 68–71 (1st Cir. 1985) (holding that an agreement to release civil rights claims against public officials in exchange for dismissal of criminal charges is per se void as against public policy), rev’d, 480 U.S. 386 (1987); Boyd v. Adams, 513 F.2d 83, 88–89 (7th Cir. 1975) (holding that release-dismissal agreements arise from inherently coercive circumstances and are invalid as against public policy in all but the rarest of circumstances); MacDonald v. Musick, 425 F.2d 373, 375–76 (9th Cir. 1970) (holding that a prosecutor cannot condition voluntary dismissal of a criminal charge upon a stipulation by the defendant that is designed to forestall the defendant’s civil suit against the police, because such conduct is unethical and a form of extortion); Dixon v. District of Columbia, 394 F.2d 966, 969 (D.C. Cir. 1968) (holding that release-dismissal agreements are inherently odious and against public policy, and that courts should have no role in promoting or enforcing them). Contra Bushnell v. Rosetti, 750 F.2d 298, 301–02 (4th Cir. 1984) (holding that a release of civil rights claims in exchange for criminal sentencing considerations should be enforced if the criminal defendant made a voluntary, deliberate, and informed decision to release the civil rights claims); Jones v. Taber, 648 F.2d 1201, 1203–04 (9th Cir. 1981) (holding, after noting that the court could find no cases on point, that the release of a civil rights claim should be governed by a voluntariness standard borrowed from maritime law).
92 394 F.2d at 969.
93 425 F.2d at 375–76 (discussing Model Code of Prof’l Responsibility DR 7-105(A) (1980), which prohibited a lawyer from presenting, participating in presenting, or threatening to present criminal charges solely to obtain an advantage in a civil matter).
94 See 480 U.S. at 392–94. A few jurisdictions impose more demanding ethical standards than the Model Code provisions, so one could argue that Rumery’s ethical approval
release-dismissal agreement is enforceable if the defendant entered into it voluntarily and intelligently, and that the public interest in enforcing the agreement outweighs the public policy that would be harmed by enforcement. The majority opinion explained both its rejection of a per se rule against enforcing release-dismissal agreements and its adoption of additional safeguards by noting that release-dismissal agreements are similar to, but distinguishable from, plea bargains. Both involve a defendant’s difficult but not unconstitutionally coercive choice to waive important rights in exchange for favorable criminal treatment. But, the Rumery majority reasoned, plea bargains of release-dismissal agreements should carry less force in those jurisdictions. See Cal. Rule of Prof’l Conduct 5-100 (1992) (prohibiting a lawyer from threatening criminal, administrative, or disciplinary charges to obtain advantage in a civil suit); Me. Bar Rule 5.6(c) (2005) (prohibiting a lawyer from presenting, or threatening to present, criminal, administrative, or disciplinary charges solely to obtain an advantage in a civil matter). On the other hand, in jurisdictions that have adopted the newer Model Rules of Professional Responsibility, the ethical question is probably moot. See ABA Comm. on Ethics and Prof’l Responsibility, Formal Op. 92-363 (1992) (discussing threats of presenting criminal charges in connection with a civil matter). The Model Rules have no specific counterpart to the Model Code’s DR 7-105(A). See id. In light of this omission, the American Bar Association’s Committee on Ethics and Professional Responsibility has opined that the Model Rules give attorneys considerably greater freedom to make such threats than did the Model Code. See id.

95 Rumery, 480 U.S. at 392–94. Although the majority agreed on the basic voluntariness standard, their fragmented opinions created some doubt about which party bears the burden of proving a release-dismissal agreement’s enforceability. See id. at 394–97 (Powell, J., concurring) (joined by Rehnquist, C.J., White, J., & Scalia, J.) (apparently implying that the party seeking to rescind the agreement should bear the burden of proof); id. at 399–401 (O’Connor, J., concurring) (arguing that the party seeking to enforce the release-dismissal agreement should bear the burden of proving its enforceability); id. at 417–20 (Stevens, J., dissenting) (joined by Brennan, Marshall, & Blackmun, J.J.) (arguing that there should be a strong presumption against the enforceability of release-dismissal agreements). The federal circuit courts interpreting Rumery on this burden of proof question generally have held that the party seeking to enforce the agreement bears the burden of proving that the agreement should be enforced. See Rodriguez v. Smithfield Packing Co., 338 F.3d 348, 353 (4th Cir. 2003) (noting that the vote of Justice O’Connor, who placed the burden of proof on the party seeking to enforce the agreement, was dispositive in Rumery); Gonzalez v. Kokot, 314 F.3d 311, 317 (7th Cir. 2002) (holding that the party seeking to enforce the agreement bears the burden of establishing its validity); Hill v. Cleveland, 12 F.3d 575, 578 (6th Cir. 1993) (same); Vallone v. Lee, 7 F.3d 196, 199 (11th Cir. 1993) (same); Cain v. Darby Borough, 7 F.3d 377, 380 (3d Cir. 1993) (same); Coughlen v. Coots, 5 F.3d 970, 974 (6th Cir. 1993) (same); Lynch v. Alhambra, 880 F.2d 1122, 1128 (9th Cir. 1989) (holding that, as to the public interest prong, the party seeking to enforce the agreement bears the burden of establishing its validity). But see Woods v. Rhodes, 994 F.2d 494, 499–502 (8th Cir. 1993) (failing to specify which party should bear the burden of proof).

96 Rumery, 480 U.S. at 395–94.

97 Id.
differ from release-dismissal agreements because a plea is conducted under judicial oversight, brings immediate and tangible benefits to the public (in particular, the rapid imposition of punishment while saving prosecutorial resources), ensures some satisfaction of the public’s interest in the prosecution of crime, and indicates through the plea colloquy that the prosecutor’s charges have some basis in fact. 98 Release-dismissal agreements often do not share these attributes. 99

Moreover, Justice O’Connor and the four dissenters agreed that the way in which release-dismissal agreements intermingle criminal justice and non-criminal justice considerations gives rise to serious concerns that should lead the courts to treat release-dismissal agreements differently from normal plea bargains. 100 According to Justice O’Connor in her concurring opinion, a release-dismissal agreement differs from a plea bargain because a release-dismissal agreement explicitly trades the public criminal justice interest in convicting law-breakers against the private financial interests of public officials in avoiding civil liability; in contrast, a prosecutor striking a valid plea bargain may consider only legitimate criminal justice concerns, such as the strength of the evidence against the defendant, the defendant’s prospects for rehabilitation, and the defendant’s degree of cooperation with the authorities. 101 When, as happens in release-dismissal agreements, the outcome of a criminal proceeding turns on extraneous considerations unrelated to criminal justice objectives, the public may lose faith in both the legitimacy of the bargaining process and the fairness of those who administer the criminal process. 102

Along similar lines, Justice Stevens and the three other dissenters argued that a release-dismissal agreement differs from a plea bargain because the delicate balance of mutual advantage that results from

---

98 Id. at 393 n.3.
99 Id. On the other hand, the plurality opined, release-dismissal agreements may serve the public interest in particular cases because such agreements can prevent public officials from wasting government time defending themselves against unjustified civil rights claims. Id. at 395–96 (plurality opinion). While emphasizing that the party seeking enforcement should bear the burden of showing that such an interest exists, Justice O’Connor agreed that this interest exists in some cases and further noted that a prosecutor’s judgment to spare the community the expense of litigation arising from minor crimes also could serve the public interest. Id. at 399–400 (O’Connor, J., concurring).
100 See id. at 400–01 (O’Connor, J., concurring); id. at 410–13 (Stevens, J., dissenting).
101 Id. at 401 (O’Connor, J., concurring). But see Gregoire v. Biddle, 177 F.2d 579, 580–81 (2d Cir. 1949) (articulating the public interest in ensuring that lawsuits do not prevent executive officials from exercising their duties).
102 Rumery, 480 U.S. at 400 (O’Connor, J., concurring).
plea bargains does not exist in release-dismissal agreements. In plea bargaining, the negotiation is a give-and-take over the nature of the defendant’s wrongdoing; in a release-dismissal agreement, the negotiation is aimed at resolving a civil rights claim against public officials that is unrelated to the nature of the defendant’s wrongdoing. Although the outcome of a criminal proceeding may affect the value of the civil claim, the two claims being negotiated in a release-dismissal agreement are quite distinct as a matter of law. Thus, the release-dismissal agreement exacts a price from the defendant unrelated to the character of his or her wrongdoing. Justice Stevens also expressed concern that in negotiating the agreement, serious public policy and ethical issues arise from the prosecutor’s representation of multiple and conflicting interests. In Rumery, then, five justices agreed that the different public policy concerns and different balance of mutual advantage that flow from release-dismissal agreements, as compared to those of normal plea bargains, justify imposing a heavier burden on the party seeking to enforce these agreements.

II. Plea Bargaining in the Enemy Combatant Context

A. The Post-9/11 Innovation of Enemy Combatant Detention

On September 11, 2001, the Al Qaeda terrorist organization attacked the United States by hijacking commercial airplanes and deliberately crashing them into the World Trade Center in New York City and the Pentagon in Washington, D.C. The attacks killed almost 3000 people—the largest loss of life the United States has ever suffered

103 Id. at 410 (Stevens, J., dissenting).
104 Id.
105 Id. at 411.
106 Id. at 412–13 (Stevens, J., dissenting).
107 Rumery, 480 U.S. at 412–13 (Stevens, J., dissenting).
108 See id. at 400–01 (O’Connor, J., concurring); id. at 410–13 (Stevens, J., dissenting). As mentioned above, the Court in Rumery did not clearly state which party bears the burden of proving a release-dismissal agreement’s enforceability, but lower courts have generally placed the burden on the party seeking to enforce the agreement. See supra note 95.
on its soil as a result of hostile attack. In response, Congress passed an Authorization for Use of Military Force resolution (the “AUMF”), which stated in relevant part:

[T]he President is authorized to use all necessary and appropriate force against those nations, organizations, or persons he determines planned, authorized, committed, or aided the terrorist attacks that occurred on September 11, 2001, or harbored such organizations or persons, in order to prevent any future acts of international terrorism against the United States by such nations, organizations or persons.

Thus began what President George W. Bush calls the “War on Terror.” As part of the War on Terror, the President has claimed the authority to designate individuals as enemy combatants and hold them under military authority for as long as the President deems necessary for national security. The power to make such designations, according to the executive branch, derives from the President’s war powers as Commander in Chief. The government asserts that detaining enemy combatants serves two military objectives: preventing these individuals from rejoining enemy forces and enabling the military to gather intelligence from the detainee. Unlike prisoner-of-war detentions in traditional wars, enemy combatant detentions in the War on Terror raise troubling new questions, including how to identify the “enemy” and how to identify the end of the conflict.

110 9/11 COMMISSION REPORT, supra note 109, at 311.
112 President George W. Bush, Address to a Joint Session of Congress and the American People (Sept. 20, 2001) (transcript available at http://www.whitehouse.gov/news/releases/2001/09/20010920-8.html) (“Our war on terror begins with al Qaeda, but it does not end there. It will not end until every terrorist group of global reach has been found, stopped and defeated.”). Although Bush Administration officials briefly re-branded this campaign as the “Global Struggle Against Violent Extremism,” President Bush has since reverted to the more forceful-sounding “War on Terror.” Eric Schmitt & Thom Shanker, New Name for ‘War on Terror’ Reflects Wider U.S. Campaign, N.Y. TIMES, July 26, 2005, at A7; Richard W. Stevenson, President Makes It Clear: The Phrase Is ‘War on Terror,’ N.Y. TIMES, Aug. 4, 2005, at A12.
113 Brief for the Respondents, supra note 3, at 16.
114 Id. at 13; see also U.S. CONST. art. II, § 2 (“The President shall be Commander in Chief of the Army and Navy of the United States.”).
115 Brief for the Respondents, supra note 3, at 15; Brief for the Petitioners, supra note 3, at 28–29.
116 See Hamdi v. Rumsfeld, 542 U.S. 507, 519–21 (2004) (recognizing that the unconventional nature of the War on Terror could lead to perpetual detentions of enemy com-
When faced with legal challenges to enemy combatant detentions, the government has argued that the President should have essentially unfettered authority to capture and imprison anyone indefinitely—whether citizen or non-citizen, captured on U.S. soil or abroad—at the sole discretion of the President as Commander in Chief.117 In 2004, the Supreme Court simultaneously issued three cases—Rasul v. Bush, Hamdi v. Rumsfeld, and Rumsfeld v. Padilla—that gave the Court an opportunity to define the scope of the President’s authority to detain enemy combatants in the War on Terror.118 These three cases provide the only existing judicial guidance on the potential limits of this novel authority.119

In the first of the 2004 enemy combatant cases, Rasul v. Bush, the Supreme Court held that the federal courts have jurisdiction to hear the habeas corpus petitions of various foreign nationals captured abroad and detained at the U.S. Naval Base in Guantanamo Bay, Cuba.120 The Court did not, however, reach the merits of the detainees’ claims.121

---

117 See Brief for the Respondents, supra note 3, at 25–27; Brief for the Petitioners, supra note 3, at 38; see also Guantanamo Detainee Cases, 355 F. Supp. 2d at 475 (noting that in response to the hypotheticals posed by the court, the government asserted that its authority to detain individuals as enemy combatants extended to a little old lady in Switzerland who writes checks to what she believes is a charity but is actually an Al Qaeda front, a person who teaches English to the son of an Al Qaeda member, and a journalist who knows the location of Al Qaeda leader Osama bin Laden but refuses to disclose it in order to protect a confidential source).


119 See Hamdi, 542 U.S. at 529–33; Rasul, 542 U.S. at 483–84; Padilla I, 542 U.S. at 451. Although prior cases involving the detention and trial of “unlawful combatants”—that is, enemy agents whom the President punishes for violating the law of war—speak to the source of the President’s power to detain combatants, they define the contours of the President’s power only as to punitive detentions, not as to the preventive, non-punitive detentions of the War on Terror. See generally In re Yamashita, 327 U.S. 1 (1945) (upholding the military trial and punishment of a Japanese general for permitting his troops to commit atrocities); Ex parte Quirin, 317 U.S. 1 (1942) (upholding the military trial and punishment of German agents who entered the United States to commit sabotage).

120 542 U.S. at 483–84.

121 See id. at 485. Since Rasul, the Supreme Court has agreed to hear a challenge to the fairness of the military tribunals taking place in Guantanamo Bay. See generally Hamdan v. Rumsfeld, 415 F.3d 33 (D.C. Cir.), cert. granted, 126 S. Ct. 622 (2005). About two months after the Supreme Court granted certiorari in Hamdan, however, Congress passed and
In the second 2004 enemy combatant case, *Hamdi v. Rumsfeld*, the Supreme Court outlined the due process guarantees for U.S. citizens captured as enemy combatants abroad. The executive branch designated Yaser Esam Hamdi, an American citizen who resided in Afghanistan during the U.S. invasion, an enemy combatant after taking him into custody in Afghanistan. The executive branch based this designation on two factors: Hamdi’s presence in Afghanistan after the U.S. invasion and the belief that Hamdi joined or assisted forces hostile to the United States or its coalition partners in Afghanistan.

Without reaching the government’s argument that the President can detain enemy combatants under his plenary authority as Commander in Chief, the Supreme Court held that Congress authorized Hamdi’s enemy combatant detention through the AUMF. Having established the President’s authority to detain Hamdi, the Court then described the process owed to an enemy combatant under the Due Process Clause of the Fifth Amendment. Applying the *Mathews v. Eldridge* balancing test, the Court held that a citizen-detainee seeking to challenge his or her classification as an enemy combatant must receive


---

122 542 U.S. at 509.
123 Id. at 510. The U.S. invaded Afghanistan under the authority of the AUMF. *Id.; see* AUMF, Pub. L. No. 107-40, § 2, 115 Stat. 224, 224 (2001) (codified at 50 U.S.C. § 1541 note (2000 & Supp. III 2003)). During the U.S. invasion, Afghan military forces allied with the United States captured Hamdi, detained him, and turned him over to U.S. troops. *Hamdi*, 542 U.S. at 510. After the U.S. government gained custody of Hamdi, officials first detained and interrogated him in Afghanistan, and again in Guantanamo Bay, until they learned that Hamdi was a U.S. citizen. *Id.* At that point, the U.S. government transferred Hamdi to a naval brig in Norfolk, Virginia. *Id.* As a result of his designation as an enemy combatant, Hamdi spent several months in U.S. military custody—held incommunicado, without being charged with any crime, and without access to counsel—before his father was able to file a habeas corpus petition on his behalf. *Id.* at 510–11.
124 *Id.* at 522 n.1, 526.
125 *Id.* at 517; *see* AUMF § 2, 115 Stat. at 224.
notice of the factual basis for that classification and a fair opportunity to rebut the government’s factual assertions before a “neutral decisionmaker.” The Court qualified its holding, however, by providing some examples of the limited process due a citizen accused of being an enemy combatant: a special military tribunal could count as a “neutral decisionmaker,” hearsay could be admissible in such a hearing, and the detainee could bear the burden of proof to rebut the government’s factual assertions. Significantly, these due process rights do not attach upon the President’s designation of the person as an enemy combatant, nor upon that person’s initial capture and detention as an enemy combatant. Instead, the Court held that the process described above is triggered by the enemy combatant’s challenge of his or her classification as part of a post-deprivation hearing reviewing whether continued detention is necessary.

In the third 2004 enemy combatant case, Rumsfeld v. Padilla (Padilla I), the Supreme Court had an opportunity to define the due process guarantees for U.S. citizens who are arrested and designated enemy combatants within the United States, but it declined to rule on the issue. Jose Padilla was a U.S. citizen whom federal authorities arrested on a material witness warrant at the Chicago O’Hare International Airport, held as a material witness in New York, and then designated an enemy combatant before he had a meaningful opportunity

---

127 Id. at 535; see Mathews v. Eldridge, 424 U.S. 319, 335 (1976). The Mathews test weighs the private interest that will be affected by the official action against the government’s interest (including the nature of the interest at stake and the burdens on the government of additional process), considering both the risk of an erroneous deprivation of that interest and the likely value of additional or substitute procedural safeguards. Mathews, 424 U.S. at 335.

128 Hamdi, 542 U.S. at 533–34, 538. By contrast, a criminal defendant—whether arrested in peace or wartime—has the right to a trial by a jury of his or her peers in which a full panoply of evidentiary protections apply, and the government must prove the defendant’s guilt beyond a reasonable doubt. See U.S. Const. amend. VI (stating that in all criminal prosecutions, the accused has the right to a speedy and public trial before an impartial jury); In re Winship, 397 U.S. 358, 361–64 (1970) (holding that under the Due Process Clause of the Fourteenth Amendment, no person may be convicted of a crime except by proof beyond a reasonable doubt); Duncan v. Kahanamoku, 327 U.S. 304, 324 (1946) (holding that because neither wartime conditions nor the declaration of martial law entitles military tribunals to supplant entirely the criminal courts within the United States, the defendants therefore were entitled to a criminal trial in a civilian court rather than in a military tribunal).

129 Hamdi, 542 U.S. at 534, 537–38.

130 See id. at 534.

131 542 U.S. at 430.
to challenge his extended detention as a material witness.\textsuperscript{132} The U.S. Court of Appeals for the Second Circuit held that the President had no authority to hold Padilla as an enemy combatant.\textsuperscript{133} Without addressing the merits of the case, the Supreme Court reversed the Second Circuit, holding that the New York court where Padilla filed his petition lacked jurisdiction to hear his habeas corpus petition.\textsuperscript{134}

After the Supreme Court's decision, Padilla renewed his litigation, this time conforming to the Court's jurisdictional requirements.\textsuperscript{135} In \textit{Padilla v. Hanft (Padilla II)}, the U.S. Court of Appeals for the Fourth Circuit relied on \textit{Hamdi} to hold that the AUMF authorized Padilla's detention—even though he was a U.S. citizen and the government neither arrested him nor designated him an enemy combatant until after he had returned to U.S. soil.\textsuperscript{136} The court reasoned that Padilla posed

\textsuperscript{132} \textit{Id.} at 430–32. Authorities arrested Padilla when he arrived in Chicago on an international flight from Pakistan and then kept him in custody as a material witness for over a month. \textit{Id.} at 430–31. Shortly before a scheduled hearing on Padilla's motion to vacate the material witness warrant, the President designated Padilla an enemy combatant, and Defense Department officials shipped Padilla to a naval brig in South Carolina. \textit{Id.} at 431–32.

\textsuperscript{133} Padilla v. Rumsfeld, 352 F.3d 695, 724 (2d Cir. 2003) (holding that the President's powers as Commander in Chief do not include the power to detain a U.S. citizen seized within the United States as an enemy combatant and that President Bush's detention of Padilla contravened the expressed will of Congress), \textit{rev'd}, 542 U.S. 426 (2004).

\textsuperscript{134} \textit{Padilla I}, 542 U.S. at 451. The majority held that because the government successfully moved Padilla from New York to South Carolina two days before his lawyer filed a habeas corpus petition on his behalf, the New York court never obtained jurisdiction over Padilla. \textit{Id.} at 441. Justice Stevens, joined by Justices Souter, Ginsburg, and Breyer, dissented, arguing that the Court should have heard Padilla's habeas petition on the merits both because of the case's profound and disturbing implications for liberty, and because the government made the change in jurisdiction a \textit{fait accompli} without providing fair notice to Padilla's attorney. \textit{See id.} at 455–65 (Stevens, J., dissenting). Justice Stevens argued that the government provided inadequate notice by vacating the material witness warrant in an \textit{ex parte} proceeding that took place on a Sunday, immediately transferring Padilla to the military facility in South Carolina, and then failing to inform Padilla's attorney officially of her client's whereabouts until after she filed the habeas petition. \textit{See id.}

\textsuperscript{135} \textit{See Brief of Petitioner for Writ of Certiorari, Padilla v. Hanft, No. 05-533 (U.S. Oct. 25, 2005), available at} 2005 WL 2822914 (appealing \textit{Padilla II}); infra note 139 and accompanying text. As a practical matter, \textit{Padilla I}'s restrictive jurisdictional requirements mean that U.S. citizen enemy combatants cannot file their habeas petitions in any jurisdiction other than the Fourth Circuit, because the government has chosen to hold U.S. citizen enemy combatants exclusively within that circuit's territorial jurisdiction. \textit{See Hamdi}, 542 U.S. at 510 (describing how upon learning of Hamdi's U.S. citizenship, the government transferred Hamdi first from Guantanamo Bay to a naval brig in Norfolk, Virginia, and then to another naval brig in Charleston, South Carolina); \textit{Padilla I}, 542 U.S. at 432 (describing how upon transferring Padilla into military custody, the government held Padilla at the Consolidated Naval Brig in Charleston, South Carolina).

the same danger to U.S. interests in Chicago as he had while abroad, so the government had the same power to designate him an enemy combatant in either circumstance. After Padilla filed a petition for certiorari appealing the Fourth Circuit’s ruling, the Justice Department unsealed a criminal indictment against Padilla in the Southern District of Florida, alleging offenses that were unrelated to and less serious than the alleged acts the government had used to justify his detention as an enemy combatant. Following an unusual series of procedural developments, the Supreme Court authorized his transfer into civilian custody and then, after some delay, denied certiorari.

137 Padilla II, 423 F.3d at 393. According to the Fourth Circuit, Padilla associated with anti-U.S. forces in Afghanistan and armed himself there in much the same way that Hamdi did, rendering him a threat similar to Hamdi. Id. at 391–92; see Hamdi, 542 U.S. at 512–13. Thus, the court reasoned, Padilla qualified as an enemy combatant for the same reasons as Hamdi. Padilla II, 423 F.3d at 392; see Hamdi, 542 U.S. at 522 n.1. And because detaining Padilla prevented his return to the battlefield, the court held that the AUMF authorized Padilla’s detention incident to the conduct of war, without specifically stating whether the war in question was the war in Afghanistan or the larger War on Terror. See Padilla II, 423 F.3d at 392; see also AUMF § 2, 115 Stat. at 224. The court characterized the Hamdi plurality’s reasoning as rendering the locus of capture irrelevant, even though the Hamdi plurality had repeatedly stated that Hamdi’s capture while in a foreign combat zone was a significant fact. Padilla II, 423 F.3d at 393–94; see Hamdi, 542 U.S. at 523–24. The court justified this result by characterizing the fact of foreign battlefield capture as merely being part of the context of the Hamdi case rather than an essential part of its reasoning. Padilla II, 423 F.3d at 393.


139 See Hanft v. Padilla (Padilla IV), 126 S. Ct. 978, 978 (2006) (mem.) (granting the application for transfer into civilian custody). In refusing authorization for the transfer, the Fourth Circuit—in an unusual display of pique—stated that the government’s actions created the impression that they were intentionally using the indictment to moot Padilla’s habeas petition and thereby evade Supreme Court review. Padilla v. Hanft (Padilla III), 432 F.3d 582, 585–86 (4th Cir. 2005), application granted by 126 S. Ct. 978 (2006). Stating that the government’s actions harmed the government’s credibility before the courts and created the impression that Padilla’s long detention was a mistake, the court held that the rule of law would best be served by maintaining the status quo and keeping the case live for consideration by the Supreme Court. Id. at 587. On January 4, 2006, the Supreme Court granted authorization for Padilla’s transfer and indicated that the Court would consider Padilla’s petition for certiorari. Padilla IV, 126 S. Ct. at 978. Three months later, a divided Court denied certiorari, with Justice Kennedy issuing a concurring opinion and Justice Ginsburg issuing a dissenting opinion. See Padilla v. Hanft (Padilla V), No. 05-533, 2006 WL 845383 (U.S. Apr. 3, 2006); id. at *2 (Kennedy, J., concurring) (describing any
B. Interaction of Enemy Combatant Detention with the Criminal Justice System

As discussed above, the Supreme Court has set very few limits on the President’s power to designate people as enemy combatants.\(^{140}\) Even in cases involving U.S. citizen enemy combatants, the Court has given the President wide latitude to arrest and hold individuals under military authority, without accusing them of any particular wrongful acts, and to keep them in custody until the War on Terror ends.\(^{141}\) And in a growing number of cases, the government has arrested alleged terrorists under civilian authority and then detained them as enemy combatants, or vice versa.\(^{142}\)

This flow between civilian prosecution and military detention is possible because the Supreme Court has accepted the government’s argument that the purpose of enemy combatant detention is to prevent fighters from taking up arms on the battlefield, not to punish them.\(^{143}\) Thus, criminal prosecution and enemy combatant detention serve different objectives and are—at least in theory—unrelated to one another.\(^{144}\) The non-punitive purpose of enemy combatant deten-

---

\(^{140}\) See Hamdi, 542 U.S. at 533–34, 538; Rasul, 542 U.S. at 485; Padilla I, 542 U.S. at 451.

\(^{141}\) See Hamdi, 542 U.S. at 533–34, 538. David Cole characterizes such detentions as effectively life sentences, asserting that society will almost certainly cure both cancer and the common cold before it can stop terrorism. Cole, supra note 5, at 41. At least one federal judge shares Cole’s concerns. See Guantanamo Detainee Cases, 335 F. Supp. 2d at 465 (noting that because the government has conceded that the War on Terror could last for several generations, detention as an enemy combatant may well amount to a life sentence).

\(^{142}\) See infra notes 146–179 and accompanying text.

\(^{143}\) Hamdi, 542 U.S. at 518 (describing enemy combatant detention as a means of preventing detainees from returning to the battlefield and taking up arms, not as a form of punishment or vengeance).

\(^{144}\) See Kansas v. Hendricks, 521 U.S. 346, 369 (1997) (holding that indefinite post-sentence civil commitment of sexually dangerous predators is not punishment because its purpose is not linked to any punitive purpose of retribution or deterrence, and therefore it does not implicate the Double Jeopardy Clause’s prohibition against punishing a defendant twice for the same offense) (discussing the Double Jeopardy Clause of U.S. Const. amend. V, which reads, “[N]or shall any person be subject for the same offence to be twice put in jeopardy of life or limb”). Yet as Justice Scalia pointed out in his dissent in Hamdi, the grounds for designating Hamdi and Padilla as enemy combatants overlapped significantly with the grounds for prosecuting a citizen for treason. Hamdi, 542 U.S. at 559–61 (Scalia, J., dissenting). Moreover, scholars have argued that, by allowing prosecutors to target allegedly dangerous individuals for their associations rather than more substantial acts, broad federal anti-terrorism laws have shifted criminal enforcement toward a more prevention-focused paradigm. See Robert M. Chesney, The Sleeper Scenario: Terrorism-Support Laws and the Demands of Prevention, 42 Harv. J. on Legis. 1, 47–75 (2005) (arguing that the
tion also suggests that a criminal defendant could be designated an enemy combatant before a scheduled trial, after the jury announces its verdict, or even during the trial.\(^{145}\)

The 2003 case of *Al-Marri v. Bush* provides one example of a person originally arrested by civilian law enforcement, but then designated an enemy combatant and transferred into military custody.\(^{146}\) In December 2001, federal agents arrested Ali Saleh Kahlahl al-Marri, first holding him as a material witness and then charging him with lying to the FBI and various forms of financial fraud.\(^{147}\) About a week before his pretrial conference, and less than a month before his scheduled trial date, the Justice Department dropped the criminal charges against al-Marri, and the Defense Department designated him an enemy combatant.\(^{148}\)

Material support of terrorism laws are an appropriate but imperfect means of prosecuting terrorists before evidence of a conspiracy exists); David Cole, *The New McCarthyism: Repeating History in the War on Terror*, 38 HARV. C.R.-C.L. L. REV. 1, 14–15 (2003) (criticizing the material support of terrorism laws as preventive law enforcement measures that make it too easy for the government to prosecute ostensibly suspicious individuals, even when there is no evidence that the person ever participated in or planned a terrorist crime). The apparent clash between present law enforcement practices and traditional theories of retribution and deterrence, however, is beyond the scope of this Note.

\(^{145}\) See Hendricks, 521 U.S. at 369 (holding that indefinite post-sentence civil commitment of sexually dangerous predators is not punishment, and therefore does not implicate the Double Jeopardy Clause’s prohibition against punishing a defendant twice for the same offense); infra notes 146–179 and accompanying text. Before the trial of September 11 co-conspirator Zacarias Moussaoui, the White House did consider dismissing the charges against him and declaring him an enemy combatant, but officials ultimately decided to let his case remain in the criminal justice system. Philip Shenon & Eric Schmitt, *White House Weighs Letting Military Tribunal Try Moussaoui, Officials Say*, N.Y. TIMES, Nov. 10, 2002, at 17.


\(^{147}\) *Al-Marri*, 274 F. Supp. 2d at 1004. The apparently non-terrorism-related criminal charges against al-Marri are an example of the Justice Department’s so-called “Al Capone” strategy of pretextual prosecution—charging terrorism defendants with lesser offenses to disrupt alleged but unproven terrorist plots. See, e.g., Cole, *supra* note 5, at 203–04 (arguing that pretextual law enforcement is potentially useful but needs to be subject to stringent judicial review to deter improper prosecutorial motives, such as racial or religious bias); Daniel C. Richman & William J. Stuntz, *Al Capone’s Revenge: An Essay on the Political Economy of Pretextual Prosecution*, 105 COLUM. L. REV. 583, 618–24 (2005) (characterizing pretextual prosecutions as a necessary tool in the War on Terror even though they can carry a high societal cost).

\(^{148}\) *Al-Marri*, 274 F. Supp. 2d at 1004. Al-Marri’s attorney, Lawrence Lustberg, told reporters that the designation was an end-run around the legal system. Schmidt, *supra* note 16, at A1. As quoted by the *Washington Post*, Lustberg believed the Administration designated al-Marri an enemy combatant because al-Marri was raising “powerful legal challenges” to the government’s allegations, and the government had no proof he was involved in terrorism. *Id.*
Another case, *United States v. Lindh*, began with military detention and ended with a guilty plea in a civilian court.\footnote{227 F. Supp. 2d 565, 569 (E.D. Va. 2002).} John Walker Lindh was a U.S. citizen—a young white man from Marin County, California—who traveled to Afghanistan in the spring of 2001.\footnote{Id. at 567–68.} Once there, he joined the Taliban regime then governing the country and obtained military training at a camp run by Al Qaeda leader Osama bin Laden.\footnote{Id.} In November 2001, during the U.S. invasion of Afghanistan, Lindh and his fighting group surrendered to Afghan troops allied with the United States in its fight against the Taliban.\footnote{Id. at 569.} The Central Intelligence Agency (the “CIA”) briefly held and interrogated Lindh but eventually turned him over to the Justice Department.\footnote{Id.} The Justice Department then charged him with a variety of criminal offenses, including providing material support to various terrorist organizations and conspiring to murder U.S. nationals.\footnote{Lindh, 227 F. Supp. 2d at 566 n.2.} On July 15, 2002, Lindh pled guilty to providing support to the Taliban and carrying an explosive during the commission of a felony, and the U.S. District Court for the Eastern District of Virginia sentenced him to twenty years' imprisonment.\footnote{Id. at 566, 572.} Interestingly, Lindh’s plea agreement included a promise by the government not to designate him an enemy combatant based on the conduct alleged in the indictment.\footnote{See infra notes 159–179 and accompanying text.}

One need not scrutinize the terms of plea agreements, however, to see that federal prosecutors have used the revolving door between civilian and military custody to their advantage.\footnote{See Plea Agreement ¶ 21, *Lindh*, 227 F. Supp. 2d 565 (No. 02-37A), available at http://files.findlaw.com/news.findlaw.com/hdocs/docs/lindh/uslindh71502pleaag.pdf.} At least two successful terrorism prosecutions—*United States v. Faris* and the “Lackawanna...
Six” case—appear to have involved direct threats to detain the defendant as an enemy combatant.158 In the Faris case, the FBI sought for questioning Iyman Faris, a thirty-four-year-old truck driver and U.S. citizen who had immigrated to Columbus, Ohio from Kashmir.159 After he agreed to cooperate on March 20, 2003, the agents interrogated Faris in a hotel room in Ohio for several days.160 With Faris’s consent, the FBI then transported him to Quantico, Virginia.161 According to Faris, the FBI subjected him to daily interrogations from 9 a.m. to 5 p.m. with a break for lunch, posted guards outside his living quarters, and permitted him to take only a one-hour escorted walk outside each night.162

Although Faris alleges that he repeatedly requested an attorney, the FBI continued interrogating him without counsel until early April 2003, when he refused to answer any questions without a lawyer present.163 On April 6, FBI agents allowed Faris to meet with his newly appointed attorney for the first time.164 On April 16, Faris’s attorney told him that if he did not accept the prosecutor’s plea offer, the FBI might send Faris to Guantanamo Bay.165 On April 17, according to Faris, an FBI agent visited him in his room and told Faris, outside the presence of his counsel, that his time to accept the plea offer was ending and that unless Faris pled guilty he might be sent to Guantanamo Bay.166 The same day, according to Faris, Faris’s attorney telephoned

158 See infra notes 159–179 and accompanying text.
161 Id. at 18–19.
163 Id. at 2–3, 6.
164 Id. at 6. Faris’s then-attorney indicated that the FBI agents introduced him to Faris. Faris Oct. 28, 2003 Hearing Transcript, supra note 12, at 8.
165 Declaration of Iyman Faris, supra note 162, at 18. During the hearing on Faris’s motion to withdraw his guilty plea, Faris’s attorney said he told Faris in mid-April that if he did not accept the plea bargain, then “there’s an agent, they’re ready to take you back to at least Columbus tonight and then perhaps Guantanamo Bay, to be decided later.” Faris Oct. 28, 2003 Hearing Transcript, supra note 12, at 10. During that hearing, the prosecutor denied threatening Faris with enemy combatant detention if he did not plead guilty, but did note that the possibility of sending Faris to Guantanamo Bay came up in a discussion with Faris’s attorney while they were driving to Quantico together. Id. at 17.
166 Declaration of Iyman Faris, supra note 162, at 18–19.
multiple times, urging him to sign the plea agreement.\footnote{Id. at 18.} Later that day, Faris signed the plea agreement and a written statement of facts, motivated in large part by his fear that the government would send him to Guantanamo Bay if he did not plead.\footnote{Id. at 19.} On May 1, he entered the plea in court.\footnote{Faris Withdrawal of Guilty Plea Appellate Brief, supra note 11, at 6; see also Statement of Facts, Faris, No. 03-CR-189 (E.D. Va. May 1, 2003), available at http://news.findlaw.com/hdocs/docs/faris/usfaris603sof.pdf.}

The next month, U.S. Attorney General John Ashcroft held a press conference alleging that Faris was involved in an aborted conspiracy to destroy the Brooklyn Bridge.\footnote{Lichtblau, supra note 11, at A1.} Meanwhile, Faris began recanting his confession, telling interrogators that what he had told them was a lie.\footnote{Declaration of Iyman Faris, supra note 162, at 22; Lichtblau, supra note 15, at A23; Jerry Markon, \textit{Ohio Man Gets 20 Years for Al Qaeda Plot; Judge Refuses to Drop Guilty Plea over Plan to Attack Brooklyn Bridge}, D.C., Wash. Post, Oct. 29, 2003, at A2. During his sentencing hearing, Faris repeatedly insisted that he was innocent. Faris Oct. 28, 2003 Hearing Transcript, supra note 12, at 41–42.} Later, Faris obtained a new attorney and attempted to challenge the voluntariness of his guilty plea, but the U.S. Court of Appeals for the Fourth Circuit denied him relief.\footnote{Faris, 388 F.3d at 457–58 (holding that Faris’s shifting story undermined his credibility as to the threat of enemy combatant detention, and suggesting in dicta that, even if prosecutors threatened Faris with detention in Guantanamo Bay, this would not undermine the voluntariness of his plea because every guilty plea necessarily involves choosing between “distasteful” options).} At the time of this writing, Faris had filed a motion to vacate his conviction for ineffective assistance of counsel.\footnote{See generally Faris 28 U.S.C. § 2255 Memorandum, supra note 13. Faris argues that his attorney provided him ineffective assistance with respect to both his decision to enter a guilty plea and his motion to withdraw the guilty plea, because the attorney failed to conduct any investigation, failed to seek any discovery from the government prior to negotiating and entering the plea, failed to prepare or file a memorandum of law in support of Faris’ motion to withdraw his guilty plea, and failed to make an adequate record at the hearing on his motion to withdraw the plea. See id. at 26–36.}

The second case involving a direct threat of enemy combatant detention was the “Lackawanna Six” case, in which the government charged six young Yemeni-American men with material support of Al Qaeda.\footnote{Michael Powell, \textit{No Choice but Guilty, Lackawanna Case Highlights Legal Tilt}, Wash. Post, July 29, 2003, at A1, available at http://www.washingtonpost.com/ac2/wp-dyn/A59245-2003Jul28.} Prosecutors characterized the men, all of whom were U.S. citizens, as a “sleeper cell” trained to carry out terrorist attacks in the
United States.\textsuperscript{175} Despite the FBI’s internal doubts about whether the men were truly as dangerous as some analysts believed, the Justice Department pushed hard on the case.\textsuperscript{176} Then-U.S. Attorney Michael Battle told the \textit{Washington Post} that his office never explicitly threatened to invoke enemy combatant status during plea negotiations, but that the defendants and their attorneys knew the Defense Department “had a hammer and an interest” and was standing ready to designate the defendants as enemy combatants.\textsuperscript{177} Patrick J. Brown, who represented one of the six accused, told the \textit{Post} that he and his fellow defense attorneys advised their clients to plead guilty because of worries that the government would respond to any defense victories in the criminal case by declaring the defendants enemy combatants.\textsuperscript{178} All six men pled guilty to providing material support to terrorists, accepting prison terms of six-and-one-half to nine years.\textsuperscript{179}

One observer has argued that this revolving door between the criminal justice system and enemy combatant detention strongly suggests that the government will use the method that is most convenient to capture a person in the first place, and then will freely turn to another form of detention on an ad hoc basis, depending on what is most advantageous for the government.\textsuperscript{180} If that argument is true—or even appears to be true—then someone accused of terrorism-related crimes could reasonably believe that if he fails to cooperate with the government by pleading guilty, he is likely to be designated an enemy combatant.\textsuperscript{181} Perhaps it should not be surprising, then,

\begin{itemize}
\item \textsuperscript{175} \textit{Id.}
\item \textsuperscript{176} \textit{See} Matthew Purdy & Lowell Bergman, \textit{Where the Trail Led: Between Evidence and Suspicion; Unclear Danger: Inside the Lackawanna Terror Case}, \textit{N.Y. Times}, Oct. 12, 2003, \S 1, at 1 (discussing the case in detail, including one FBI agent’s assessment that he did not see the defendant he interviewed as being a potential suicide bomber, but merely “an all-American kid who loves so much what he has in America and, for some reason, somehow he got involved in this”).
\item \textsuperscript{178} Powell, \textit{supra} note 174, at A1.
\item \textsuperscript{179} \textit{Id.}
\item \textsuperscript{180} \textit{See} Radack, \textit{supra} note 6, at 541. According to Jesselyn Radack, who coined the “revolving door” metaphor, moving terrorism defendants back and forth between the criminal justice system and enemy combatant detention is a particularly noxious variety of forum-shopping that makes enemy combatant detentions appear to be situational detentions of convenience rather than detentions on the merits and undermines the legitimacy of both the criminal justice system and the military system. \textit{Id.}
\item \textsuperscript{181} \textit{See id.}\
\end{itemize}
that in the eleven terrorism prosecutions the Justice Department has cited as major successes in its annual reports between 2002 and 2004, all but two of the cases terminated with most or all of the defendants choosing to plead guilty.\textsuperscript{182}

III. Analysis: Enemy Combatant Threat Bargains Should Be Per Se Unenforceable

Is a prosecutor’s threat, during plea negotiations, to detain the defendant as an enemy combatant akin to the permissible threats of imposing heavier sentences or bringing new indictments against the defendant?\textsuperscript{183} If so, then any terrorism defendant who seeks to invalidate an enemy combatant threat bargain must show that fear of enemy combatant detention so tightly gripped the defendant that, even with the assistance of counsel, the defendant could not make a rational decision.\textsuperscript{184}

The threat of enemy combatant detention is, however, sui generis, and should not be treated like normal plea bargaining tactics for two major reasons.\textsuperscript{185} First, enemy combatant threat bargains do not arise from the normal give-and-take of plea bargaining because the choice between a plea bargain and extrajudicial enemy combatant detention—with its limited due process guarantees, unusual severity, and unrelatedness to criminal justice objectives—creates extraordinary pressure to plead guilty to a degree unlike that presented by normal plea bargaining threats.\textsuperscript{186} Second, enemy combatant threat bargains create serious public policy concerns and serve few societal interests because


\textsuperscript{184} See Brady, 397 U.S. at 750.

\textsuperscript{185} See infra notes 186–255 and accompanying text.

\textsuperscript{186} See infra notes 189–216 and accompanying text.
they lack the mutuality of benefits that characterizes normal plea bargains, substantially increase the chance that innocent defendants will plead guilty, serve no societal interests that could not be served equally well by other means, and threaten both the integrity of the criminal justice system and the rule of law. Thus, the most appropriate judicial response is to hold enemy combatant threat bargains per se unenforceable under the Due Process Clause of the Fifth Amendment.

A. Enemy Combatant Threat Bargains Distinguished from the Normal Give-and-Take of Plea Bargaining

In a normal plea bargaining situation, the prosecutor tries to convince the defendant to plead guilty by emphasizing the consequences of a guilty verdict for the crime charged or by threatening to seek a new indictment against the defendant. In both such situations, the alternative to accepting the plea bargain is going to trial. If the defendant is guilty, then the two choices the prosecutor offers to the defendant—the bargain or the trial—both directly serve criminal justice objectives, because both seek to punish and reform the defendant based on his or her past bad acts. This is the backdrop against which the U.S. Supreme Court decided to enforce the plea bargains in Brady v. United States and its progeny. In contrast, when a prosecutor tries to convince a defendant to plead guilty by threatening the defendant with enemy combatant status, the prosecutor is not comparing the consequences of a plea bargain to those of a criminal jury trial; rather, the

---

187 See infra notes 217–255 and accompanying text.
189 See Hayes, 434 U.S. at 364–65; Brady, 397 U.S. at 750.
190 See, e.g., Hayes, 434 U.S. at 365; Brady, 397 U.S. at 750.
191 See Town of Newton v. Rumery, 480 U.S. 386, 400–01 (1987) (O’Connor, J., concurring); id. at 410 (Stevens, J., dissenting); Hayes, 434 U.S. at 364–65; Brady, 397 U.S. at 750. If, on the other hand, the defendant is not guilty, then the trial is likely to serve the important criminal justice objective of exonerating the innocent. See Berger v. United States, 295 U.S. 78, 88 (1935) (describing the U.S. Attorney’s obligation both to prevent the guilty from escaping and to refrain from making the innocent suffer).
192 See Hayes, 434 U.S. at 364–65; Parker, 397 U.S. at 794–97; Richardson, 397 U.S. at 768–70; Brady, 397 U.S. at 750–51.
consequences of a plea bargain are weighed against those of the extrajudicial black hole of enemy combatant detention.\footnote{See Hamdi v. Rumsfeld, 542 U.S. 507, 533–35 (2004) (describing the extremely limited process that is due to an enemy combatant).}

For three reasons, the threat of enemy combatant detention creates extraordinary pressure to plead guilty that is unlike the pressures of any traditional plea bargaining tactic.\footnote{See infra notes 199–213 and accompanying text.} First, the process due to a defendant in enemy combatant detention is uniquely unlike that due to a defendant in a criminal trial.\footnote{See infra notes 199–205 and accompanying text.} Second, the consequences of being designated an enemy combatant are unusually severe.\footnote{See infra notes 206–209 and accompanying text.} Third, the threat of enemy combatant detention imports an extra element into plea negotiations that is unrelated to criminal justice objectives.\footnote{See infra notes 210–213 and accompanying text.} Consequently, the policy reasoning and basic assumptions that underlie \textit{Bordenkircher v. Hayes}, \textit{Brady}, and other typical plea bargaining cases should not apply to enemy combatant threat bargains.\footnote{See Hayes, 434 U.S. at 364–65; Parker, 397 U.S. at 794–97; Richardson, 397 U.S. at 768–70; Brady, 397 U.S. at 750–51.}

First, the process due to a detainee in enemy combatant detention is uniquely unlike that due to a defendant in a criminal trial.\footnote{See Hamdi, 542 U.S. at 533–35.} In a criminal trial, the government must prove the defendant guilty beyond a reasonable doubt.\footnote{In re Winship, 397 U.S. 358, 364 (1970) (holding that under the Due Process Clause of the Fourteenth Amendment, no person may be convicted of a crime except by proof beyond a reasonable doubt).} In enemy combatant detention, by contrast, the detainee becomes an enemy combatant as soon as the President designates the person as such, and the detainee bears the burden of \textit{disproving} the government’s factual allegations in any subsequent legal challenge.\footnote{Hamdi, 542 U.S. at 534.} In a criminal trial, the defendant has the right to be tried before a jury of his or her peers in a civilian court.\footnote{See Duncan v. Kahanamoku, 327 U.S. 304, 319–24 (1946) (holding that because neither wartime conditions nor the declaration of martial law entitles military tribunals to supplant entirely the criminal courts, civilian defendants accused of crimes are entitled to a criminal trial in a civilian court rather than in a military tribunal); \textit{Ex parte Milligan}, 71 U.S. 2, 119–24 (1866) (holding that a military commission, in a state that is not in rebellion and where the courts are open and unobstructed, has no jurisdiction to try a defendant and that the use of such a tribunal violated the defendant’s Fifth and Sixth Amendment rights by denying him a jury trial in a civilian court).} But in enemy combatant detention, the detainee’s challenge may take place
in a military tribunal. In a criminal trial, the government may not prove its case by introducing hearsay and evidence that poses too great a risk of unfair prejudice. In enemy combatant detention, however, the government may use hearsay against the detainee and generally may dispense with other evidentiary procedures that the government finds overly burdensome.

In addition, the consequences of being designated an enemy combatant are unusually severe. As the result of a guilty plea or guilty verdict at trial, the criminal defendant receives a definite sentence, and the defendant’s treatment is limited by the Eighth Amendment right to be free from cruel and unusual punishment. As the result of being designated an enemy combatant, the detainee faces many of the same harms as a convict (for example, imprisonment and damage to reputation), but additionally faces an indefinite period of confinement, and the Eighth Amendment prohibition against cruel and unusual punishment might not impose any limitations on the conditions of confinement. Because enemy combatant detention involves a potentially lifelong confinement of uncertain length, in unusually restrictive con-

---

203 Hamdi, 542 U.S. at 538.
204 See, e.g., Fed. R. Evid. 403 (making evidence inadmissible if its probative value is substantially outweighed by the danger of unfair prejudice); Fed. R. Evid. 802 (making hearsay inadmissible); Crawford v. Washington, 541 U.S. 36, 54–68 (2004) (holding that the Confrontation Clause bars prosecutors from introducing the testimonial statements of any witness who does not appear at trial, unless the witness is unavailable and the defendant had a prior opportunity to cross-examine the witness).
205 Hamdi, 542 U.S. at 533–54.
207 See U.S. Const. amend. VIII (prohibiting cruel and unusual punishment); Fed. R. Crim. P. 32. (describing federal sentencing procedures).
208 See Riggins v. Nevada, 504 U.S. 127, 133 (1992) (reserving the issue of whether the Eighth Amendment imposes any limits on the involuntary administration of antipsychotic drugs to a pretrial prisoner, as opposed to a convicted prisoner); Ingraham v. Wright, 430 U.S. 651, 664–71 (1977) (declining to extend the Eighth Amendment’s prohibition against cruel and unusual punishment to encompass schoolhouse discipline because the Eighth Amendment historically applied only to post-conviction punishment of criminals); In re Guantanamo Detainee Cases, 355 F. Supp. 2d 443, 465–66 (D.D.C. 2005) (noting that for enemy combatants, the uncertain and potentially lifelong nature of their confinement may make enemy combatant detention an even worse deprivation of liberty than being tried, convicted, and sentenced to a fixed term of imprisonment); Ctr. for Nat’l Sec. Studies v. U.S. Dep’t of Justice, 215 F. Supp. 2d 94, 105 (D.D.C. 2002) (acknowledging the government’s contention that persons detained in connection with the September 11 attacks face embarrassment, humiliation, risk of retaliation, harassment, and physical harm due to having their names connected to the attacks), aff’d in part and rev’d in part, 331 F.3d 918 (D.C. Cir. 2003), cert. denied, 540 U.S. 1104 (2004).
ditions, it is more extreme than a life sentence imposed after a criminal trial and conviction.\textsuperscript{209}

Lastly, the threat of enemy combatant detention is unrelated to criminal justice objectives.\textsuperscript{210} In normal plea bargains, both possible outcomes—the prosecutor’s offers and the threatened trial—serve an important criminal justice objective of punishing guilty defendants’ past bad acts (or, in the case of innocent defendants, allowing them the opportunity to exonerate themselves).\textsuperscript{211} In contrast, the two purposes of enemy combatant detention are to facilitate interrogation and to prevent the detainee from returning to the battlefield.\textsuperscript{212} Enemy combatant detention is preventive, not punitive, detention, and thus it is unrelated to the criminal justice objective of punishing criminals for past acts.\textsuperscript{213}

As a result of these differences, introducing the threat of enemy combatant detention into plea bargaining disrupts the normal give-and-take of plea bargaining.\textsuperscript{214} Hayes, Brady, and their progeny all dealt with situations in which the threats formed part of that normal give-and-take.\textsuperscript{215} Their reasoning should not apply to the enemy combatant threat scenario because the threat of enemy combatant detention—with its limited due process guarantees, stark differences from a criminal trial, and unrelatedness to criminal justice objectives—is a world apart from the traditional threats identified in Hayes, Brady, and other typical plea bargaining cases.\textsuperscript{216}

B. \textit{Public Policy Concerns and the Failure to Serve Societal Interests}

In general, the Supreme Court places a high value on preserving the finality of plea bargains, reasoning that refusing to enforce plea bargains arising from the threat of new indictments, inaccurate legal advice, fear of the death penalty, or coerced confessions would en-

\textsuperscript{210} Hamdi, 542 U.S. at 518.
\textsuperscript{211} See Rumery, 480 U.S. at 400–01 (O’Connor, J., concurring); id. at 410 (Stevens, J., dissenting).
\textsuperscript{212} Brief for the Respondents, \textit{supra} note 3, at 15; Brief for the Petitioners, \textit{supra} note 3, at 28–29.
\textsuperscript{213} Hamdi, 542 U.S. at 518.
\textsuperscript{214} See Hayes, 434 U.S. at 364–65; Parker, 397 U.S. at 794–97; Richardson, 397 U.S. at 768–70; Brady, 397 U.S. at 750–51.
\textsuperscript{215} See Hayes, 434 U.S. at 364–65; Parker, 397 U.S. at 794–97; Richardson, 397 U.S. at 768–70; Brady, 397 U.S. at 750–51.
\textsuperscript{216} See Hayes, 434 U.S. at 364–65; Parker, 397 U.S. at 794–97; Richardson, 397 U.S. at 768–70; Brady, 397 U.S. at 750–51.
danger the viability of all plea bargaining.\textsuperscript{217} The mutual benefits that plea bargaining normally creates for both parties create a strong public policy reason to preserve their finality.\textsuperscript{218} \textit{Town of Newton v. Rumery} teaches, however, that when a particular kind of plea bargain gives rise to unusual and serious public policy concerns, such as in release-dismissal agreements, the courts may judge its enforceability by a different standard.\textsuperscript{219} Enemy combatant threat bargains raise unusual and serious public policy concerns—indeed, concerns markedly more serious than those the Court addressed in \textit{Rumery}.\textsuperscript{220} Thus, the severe consequences of enforcing enemy combatant threat bargains outweigh the limited extent to which they serve the general public policy reasons for preserving plea bargains.\textsuperscript{221}

First, enemy combatant threat bargains lack the mutuality of interests that characterizes normal plea bargains.\textsuperscript{222} Compared with a trial, a plea bargain allows the government to save scarce judicial resources and secure a prompt punishment.\textsuperscript{223} The defendant, meanwhile, benefits by limiting his or her potential sentence and avoiding the burdens of a trial.\textsuperscript{224} But when a plea bargain is compared to the extrajudicial black hole of enemy combatant detention, the balance of interests is very different from both the government’s perspective and the defendant’s perspective.\textsuperscript{225}

From the government’s perspective, an enemy combatant threat bargain serves the government’s interests no better than enemy combatant detention.\textsuperscript{226} Regardless of whether the defendant accepts the bargain or chooses to be detained as an enemy combatant, the gov-

\textsuperscript{217} See Hoyes, 434 U.S. at 364–65; Parker, 397 U.S. at 794–97; Richardson, 397 U.S. at 768–70; Brady, 397 U.S. at 750–51.

\textsuperscript{218} See Brady, 397 U.S. at 752–53. As the result of a plea bargain, the state saves scarce judicial resources and obtains prompt punishment, and the defendant limits his exposure and avoids the burdens of a trial. Id. at 752.

\textsuperscript{219} See 480 U.S. at 393–94; id. at 400–01 (O’Connor, J., concurring); id. at 408–11 (Stevens, I., dissenting).

\textsuperscript{220} See id. at 393–94 (majority opinion); id. at 400–01 (O’Connor, J., concurring); id. at 408–11 (Stevens, J., dissenting).

\textsuperscript{221} See Santobello v. New York, 404 U.S. 257, 261 (1971) (describing the benefits that plea bargaining provides to society as a whole); Brady, 397 U.S. at 752–53 (describing the mutuality of benefits that legitimates plea bargaining).

\textsuperscript{222} See Brady, 397 U.S. at 752–53.

\textsuperscript{223} Id.

\textsuperscript{224} Id.

\textsuperscript{225} See infra notes 226–236 and accompanying text.

\textsuperscript{226} See infra note 227 and accompanying text.
ernment expends few judicial resources, achieves a prompt resolution, and successfully imprisons the defendant. 227

From the defendant’s perspective, however, introducing the threat of enemy combatant detention throws the traditional balance of interests out the window and makes pleading guilty the only rational choice. 228 If the defendant rejects the plea bargain and is designated an enemy combatant, there is no burden of proof for the defendant to waive. 229 There is no right against self-incrimination to waive. 230 There is no jury trial to waive. 231 There is no right of confrontation to waive. 232 Thus, the government offers the defendant a choice only in that the defendant may choose between waiving these rights himself, or watching the government take these rights away. 233 From the defendant’s perspective, this perverts the plea negotiations into the old children’s trick, “heads I win, tails you lose.” 234 Indeed, a

---

227 Compare Hamdi, 542 U.S. at 531–32 (describing the government interests that the Court has sought to accommodate in determining the due process standards for enemy combatant detention), with Santobello, 404 U.S. at 260 (describing the government interests in plea bargaining). Also, if the defendant has committed only minor crimes or no crimes at all, then the bargain may actually work against the government’s interest in imposing a punishment proportional to the defendant’s wrongdoing. See U.S. Dep’t of Justice, United States Attorneys’ Manual: Title 9, Criminal Division § 9-27.400B (2002) (instructing federal prosecutors that plea bargaining should honestly reflect the totality and seriousness of the defendant’s conduct), available at http://www.usdoj.gov/usao/ousa/foia_reading_room/usam/title9/27mcrm.htm#9-27.400; see also Berger, 295 U.S. at 88 (emphasizing that the U.S. Attorney’s interest in a criminal prosecution is not merely to win convictions, but also to serve the broader goals of justice); Model Penal Code § 1.02(2)(c) (1962) (describing one of the goals of the Model Penal Code as seeking to avoid excessive, disproportionate, or arbitrary punishments).

228 See infra notes 229–236 and accompanying text.

229 See Hamdi, 542 U.S. at 534 (holding that when a person challenges his or her classification as an enemy combatant, the person may bear the burden of proving his or her innocence).

230 See Chavez v. Martinez, 538 U.S. 760, 769–70 (2003) (plurality opinion) (stating that where police shot a suspect multiple times, arrested him, and then coercively interrogated him in the ambulance and the emergency room, the state did not violate his Fifth Amendment right against self-incrimination because none of the compelled statements were used against him in any subsequent criminal proceeding). Because enemy combatant detention is not a form of punishment and does not terminate in a criminal proceeding, one could argue that Chavez v. Martinez would govern the applicability of the Fifth Amendment to enemy combatant detention. See Hamdi, 542 U.S. at 518; Martinez, 538 U.S. at 769–70.

231 See Hamdi, 542 U.S. at 538 (holding that when a person challenges his or her classification as an enemy combatant, a military tribunal is a permissible venue).

232 See id. at 533–34, 538 (holding that when a person challenges his or her classification as an enemy combatant, hearsay and affidavit evidence are permissible).

233 See id. at 518, 534, 538; Martinez, 538 U.S. at 769–70.

defendant who refuses to plead guilty loses several significant rights that a convicted felon retains, such as a sentence of definite length, freedom from cruel and unusual treatment, and the right to visits from attorneys.235 This illusory choice makes the Fifth, Sixth, and Seventh Amendments mere hollow promises, and it eliminates the mutuality of interests that has traditionally legitimated plea bargaining.236

Second, applying Brady standards to enemy combatant threat bargains would legitimize these extraordinarily coercive circumstances and thereby substantially increase the likelihood that innocent defendants will choose to plead guilty.237 The choice between pleading guilty and being designated an enemy combatant leaves no opportunity for the defendant to force the government to make its proof; rather, the defendant merely has a choice between two kinds of detention.238 Given this choice, only the hardiest (or foolhardiest) of defendants would reject the plea bargain and opt to be designated an enemy combatant.239 The very structure of the arrangement is so coercive that it invites perjury in the form of false guilty pleas.240 In other contexts,

---


236 See Ex parte Milligan, 71 U.S. at 123–24 (opining that allowing military justice to supplant the common law courts would make democracy a failure and put an end to liberty).

237 See Brady, 397 U.S. at 758 (noting that the Court might have reached a different result had the tactic in question substantially increased the likelihood that defendants would falsely plead guilty).

238 See Hamdi, 542 U.S. at 534 (holding that when a person challenges his or her classification as an enemy combatant, the person may bear the burden of proving his or her innocence).

239 See Perry, 417 U.S. at 28 (emphasizing that if the prosecutor can easily use new indictments to “up[] the ante” whenever a defendant appeals, then only the hardiest of defendants will choose to exercise his or her right to appeal).

240 See United States v. Waterman, 732 F.2d 1527, 1531–33 (8th Cir. 1984) (en banc, with an equally divided court) (reversing the defendant’s conviction because a prosecution witness’s plea agreement promised the witness a favorable sentencing recommendation contingent upon the results of his testimony); United States v. Dailey, 589 F. Supp. 561, 564–65 (D. Mass. 1984) (holding that a plea agreement that made a witness’s sentencing recommendation contingent upon the successful prosecution violated due process), rev’d, 759 F.2d 192 (1st Cir. 1985) (holding that the court below misread the language of the agreement and that the agreement did not make the sentencing recommendation contingent upon the government’s successful use of the proffered testimony).
courts have refused to countenance plea agreements that invite per-
jury; the courts should do so in this context as well.241

Third, enforcing enemy combatant threat bargains serves no le-
gitimate governmental interest that could not be served equally well
merely by designating those who deserve to be enemy combatants as
enemy combatants in the first place.242 As described above, both en-
emy combatant detention and plea bargains lead to limited expendi-
ture of judicial resources, prompt resolution, and imprisonment of
the defendant.243 From the government’s perspective, the only benefit
that a defendant’s guilty plea has over enemy combatant detention is
that the widespread use of enemy combatant detention would be pol-
itically untenable, whereas frequent criminal convictions of suspected
terrorists are likely to be popular.244 Popularity, however, is not the
kind of interest that a court should weigh in the government’s fa-
vor.245

Finally, court enforcement of enemy combatant threat bargains
undermines the rule of law and wrongly rewards the President for
clothing military detention in civilian trappings.246 As the Supreme

241 See Waterman, 732 F.2d at 1531–33; Dailey, 589 F. Supp. at 564–65. As Justice Suther-
land famously stated in Berger v. United States, a federal prosecutor’s interest in a criminal
prosecution is not merely to win convictions, but to do justice. See 295 U.S. at 88. Though
the prosecutor “may strike hard blows, he is not at liberty to strike foul ones. It is as much
his duty to refrain from improper methods calculated to produce a wrongful conviction as
it is to use every legitimate means to bring about a just one.” Id.

242 See Hamdi, 542 U.S. at 531–32 (describing the government interests that the Court
has sought to accommodate in determining due process standards for enemy combatant
detention); Santobello, 404 U.S. at 260 (describing the government interests in plea bar-
gaining).

243 See Hamdi, 542 U.S. at 531–32; Santobello, 404 U.S. at 260.

244 See Cole, supra note 5, at 46 (noting that enemy combatant detention has received
far more criticism than many other anti-terrorism measures that threaten civil liberties);
President George W. Bush, President Discusses Patriot Act (June 9, 2005) (transcript avail-
that the Justice Department has made communities safer by filing criminal charges against
more than 400 terrorism suspects and convicting more than half of those charged).

245 See United States v. Eichman, 496 U.S. 310, 318 (1990) (holding that popular oppo-
sition to flag burning did not increase the government’s interest in suppressing that form
of speech); Cooper v. Aaron, 358 U.S. 1, 16 (1958) (holding that segregationists’ threats of
mob violence did not justify denying black schoolchildren the right to attend integrated
schools); see also W. Va. State Bd. of Educ. v. Barnette, 319 U.S. 624, 638 (1942) (“The very
purpose of a Bill of Rights was to withdraw certain subjects from the vicissitudes of political
controversy, to place them beyond the reach of majorities and officials and to establish
them as legal principles to be applied by the courts.”).

246 See Korematsu v. United States, 323 U.S. 214, 248 (1944) (Jackson, J., dissenting)
(arguing that the courts should not carry out a military expedient that has no place in law
Court recognized in *Boykin v. Alabama*, a plea bargain can become a “perfect cover-up of unconstitutionality.” This is especially true when the plea bargain covers up the quiet pressure that military authority exerts on a criminal defendant. Enemy combatant detention serves very different objectives from imprisonment of criminals. The former is a preventive detention for national security purposes, and the latter punishes the defendant for his or her past violations of the law. Such military authority is dangerous enough on its own, because military detention of civilians in lieu of criminal prosecution is generally hostile to the Anglo-American legal tradition; its very flexibility invites abuse of power. But these dangers multiply when courts let the wolf of wartime powers slip into the sheep’s clothing of the judicial system. As Justice Robert Jackson wisely observed in his dissent to the World War II internment case of *Korematsu v. United States*, the courts must exercise only the judicial power, applying law and abiding by the Constitution, lest they lose their identity as civil courts and become instruments of military policy. Whenever a court enforces an enemy combatant threat bargain, the court turns

under the Constitution); *Ex parte Milligan*, 71 U.S. at 121 (holding that a military tribunal cannot derive its authority from the judicial power).


248 See *Korematsu*, 323 U.S. at 246 (Jackson, J., dissenting) (arguing that when a military commander does something unconstitutional, it is an incident, but when the courts approve of it, that incident becomes constitutional doctrine).

249 See *Hamdi*, 542 U.S. at 518 (describing enemy combatant detention as a means of preventing detainees from returning to the battlefield and taking up arms, not a form of punishment or vengeance); Declaration of Vice Admiral Lowell E. Jacoby, supra note 235, reprinted in Joint App. at 86 (describing the importance for national security of detaining Padilla for interrogation purposes).

250 See *Hamdi*, 542 U.S. at 518.

251 See id. at 559–69 (Scalia, J., dissenting) (arguing that, absent suspension of the writ of habeas corpus, the Founding Fathers never intended to grant the military the power to detain citizens without trial); *Ex parte Milligan*, 71 U.S. at 121–24 (holding that military detention can never be applied to citizens in non-rebel states where the courts are open and unobstructed, because civil liberty and this kind of martial law cannot coexist); cf. *Korematsu*, 323 U.S. at 220 (noting that in wartime circumstances of great peril, the government may take actions that are inconsistent with the United States’ basic governmental institutions); id. at 224 (Frankfurter, J., concurring) (arguing that the government may take actions under the war power that would be condemned as lawless in other contexts).

252 See *Korematsu*, 323 U.S. at 245–46 (Jackson, J., dissenting) (arguing that judicial approval of the internment of Japanese Americans struck a deeper blow to liberty than the military internment order itself, because when a judicial opinion puts the imprimatur of constitutionality on a military order, the court has validated the principle for all time, leaving it lying about “like a loaded weapon ready for the hand of any authority that can bring forward a plausible claim of an urgent need”).

253 Id. at 247.
plea bargaining—and therefore the courts themselves—into an instrument of military policy.\footnote{254\ See id.} Such intermingling of military and judicial roles threatens the integrity of the criminal justice system and poses grave threats to the rule of law.\footnote{255\ See Duncan, 327 U.S. at 320–22 (describing the view of the Founding Fathers that military power must not be permitted to interfere with civilian government, and particularly the judiciary).}

C. The Need for Per Se Unenforceability

Enemy combatant threat bargains do not arise from the normal give-and-take of plea bargaining, they create serious public policy concerns, and they serve few, if any, societal interests.\footnote{256\ See supra notes 189–255 and accompanying text.} Thus, the standards for enforcement of normal plea bargains should not apply to enemy combatant threat bargains.\footnote{257\ See Rumery, 480 U.S. at 400–01 (O’Connor, J., concurring); id. at 410–13 (Stevens, J., dissenting).} Rumery’s tougher standards for enforcing release-dismissal agreements also fail to protect adequately the defendant’s right to due process of law.\footnote{258\ See infra notes 260–265 and accompanying text. See generally Rumery, 480 U.S. 386.} Instead, it is most appropriate to apply the reasoning of United States v. Jackson, North Carolina v. Pearce, and Blackledge v. Perry to invalidate enemy combatant threat bargains.\footnote{259\ See Perry, 417 U.S. at 27–29 (holding that the prosecutor’s indictment of the defendant on felony charges in response to the defendant’s appeal of a misdemeanor conviction imposed unconstitutional pressure discouraging the defendant from appealing); North Carolina v. Pearce, 395 U.S. 711, 723–24 (1969) (holding that a judge’s imposition of heavier sentences upon re-trial chilled defendants’ exercise of the right to appeal); Jackson, 390 U.S. at 583–85 (holding the death-by-jury, life-by-plea structure of the statute unconstitutional because it penalized defendants for exercising their Sixth Amendment right to demand a jury trial).}

Rumery’s release-dismissal standard—the defendant must have entered into the agreement voluntarily and intelligently, and the public interest in enforcing the agreement must outweigh the public policy harmed by enforcement—is not appropriate for the enemy combatant threat bargain context.\footnote{260\ See Rumery, 480 U.S. at 401–02 (O’Connor, J., concurring).} The Rumery standard relies upon a careful, case-by-case factual inquiry into the public interest in enforcing the agreement.\footnote{261\ See id. at 392, 397–98 (majority opinion).} But under Hamdi v. Rumsfeld, the government’s conclusory affidavits attesting to the defendant’s dangerousness are an adequate basis for designating the defendant an enemy combat-
Thus, to evaluate the public interest in enforcing an enemy combatant threat bargain, the court would have to rely solely on the factual assertions in the government’s conclusory affidavits, with no way of probing those assertions. An inquiry so starved of facts would not satisfy Rumery’s demand for case-by-case decision making. Moreover, if history is any guide, a court’s unquestioning reliance on the government’s uncorroborated factual assertions would very likely lead to injustice.

In addition, the government’s primary interest in enforcing the plea bargain—to prevent dangerous terrorists from carrying out attacks by keeping them detained—is actually illusory. If the threat of enemy combatant designation is truly justified, then the government could just as easily remove the defendant from the streets by designating the defendant an enemy combatant in the first place. And if the

---

262 See Hamdi, 542 U.S. at 538.
263 See id.; Rumery, 480 U.S. at 392, 397–98.
264 See Rumery, 480 U.S. at 397–98 (endorsing a case-by-case approach for examining the enforceability of release-dismissal agreements); id. at 401–02 (O’Connor, J., concurring) (describing the close examination of many factors that indicates whether or not a release-dismissal agreement should be enforced).
265 See, e.g., Korematsu, 323 U.S. at 223–24 (upholding Korematsu’s conviction for violating the race-based wartime exclusion orders); Hirabayashi v. United States, 320 U.S. 81, 102 (1943) (upholding Hirabayashi’s conviction for violating the race-based wartime curfew orders). The most infamous illustration of the perils of such reliance comes from the World War II Japanese American internment cases of Korematsu v. United States and Hirabayashi v. United States, in which the Supreme Court relied on the factual conclusions of an Army report to uphold race-based curfews and exclusion of Japanese Americans as necessary military measures. See Korematsu, 323 U.S. at 217–24; Hirabayashi, 320 U.S. at 100–05. Nearly half a century after the internment program ended, historical researchers discovered that the report was a knowing and deliberate misrepresentation; War Department officials had doctored the report in order to assist with the internment litigation and then suppressed evidence of their misrepresentation. See Hirabayashi v. United States, 828 F.2d 591, 593–99 (9th Cir. 1987) (evaluating Hirabayashi’s petition for a writ of error coram nobis to set aside his conviction due to manifest injustice); Korematsu v. United States, 584 F. Supp. 1406, 1416–19 (N.D. Cal. 1984) (evaluating Korematsu’s petition for a writ of error coram nobis to set aside his conviction due to manifest injustice). In the mid-1980s, lower courts acknowledged this injustice by vacating the wartime criminal convictions of two of the Japanese Americans who had violated the race-based military orders. See Hirabayashi, 828 F.2d at 608 (vacating Hirabayashi’s wartime conviction); Korematsu, 584 F. Supp. at 1420 (vacating Korematsu’s wartime conviction). More recent examples of such government prevarication also exist. See United States v. Wilson, 289 F. Supp. 2d 801, 807–17 (S.D. Tex. 2003) (vacating a former CIA official’s criminal conviction for exporting explosives to Libya because the government knowingly introduced a false affidavit by the executive director of the CIA that prejudiced his defense).
266 See id. Of course, numerous distinguished scholars and jurists have convincingly argued that threatening a U.S. citizen with enemy combatant detention is never justified ab-
threat of enemy combatant designation is not justified, then the government has no legitimate interest in detaining the person other than by normal criminal processes.268

The inability of the courts to conduct an in-depth analysis of the public interest in enforcement, as well as the very serious liberty, due process, and judicial integrity interests harmed by enforcement, counsel for a per se rule against enforcement of enemy combatant threat bargains.269 There is constitutional support for such a rule.270 Like the statutory structure in Jackson, the judge’s resentencing in Pearce, and the prosecutor’s reindictment in Perry, threats of enemy combatant detention during plea bargaining violate the Due Process Clause of the Fifth Amendment because they chill the exercise of a defendant’s right to a jury trial, deterring all but the hardest defendants from refusing the proffered plea bargain.271 In order to prevent these due process violations from taking place, courts should refuse to enforce enemy combatant threat bargains.272

This per se rule does not interfere with the enforcement of normal plea bargains because the policy reasoning behind normal plea bargaining decisions does not apply to enemy combatant threat bargains.273 First, the policy reasoning behind normal plea bargaining decisions such as Brady and Hayes is inapplicable because enemy combatant threat bargains are so clearly distinguishable from the traditional give-and-take of plea bargaining.274 Threats of enemy combatant detention are more akin to the unconstitutional threats that the Court condemned in Pearce and Perry.275 Second, enemy combatant detention is itself unique.276 Enemy combatant detention—a potentially lifelong confinement of uncertain length, in unusually restrictive

---


269 See Rumey, 480 U.S. at 392, 397–98.

270 See Perry, 417 U.S. at 27–29; Pearce, 395 U.S. at 725

271 See Perry, 417 U.S. at 27–29; Pearce, 395 U.S. at 725; Jackson, 390 U.S. at 583.

272 See Perry, 417 U.S. at 27–29; Pearce, 395 U.S. at 725.

273 See Corbitt v. New Jersey, 439 U.S. 212, 212–13 (1978); Hayes, 434 U.S. at 364–65; Parker, 397 U.S. at 794–97; Richardson, 397 U.S. at 768–70; Brady, 397 U.S. at 750–51.

274 See Hayes, 434 U.S. at 364–65; Parker, 397 U.S. at 794–97; Richardson, 397 U.S. at 768–70; Brady, 397 U.S. at 750–51.

275 See Perry, 417 U.S. at 27–29; Pearce, 395 U.S. at 723–24.

conditions—is an unusually severe form of detention, more extreme than a life sentence imposed after a trial and conviction, and it arises from a process where confinement is a much more certain outcome than that of any criminal trial.\textsuperscript{277}

This rule of per se unenforceability should apply regardless of a prosecutor’s motivation for making the detention threat.\textsuperscript{278} As the Court stated in \textit{Perry}, a defendant is entitled to pursue his or her constitutional rights without fear of government retaliation, no matter what the government’s motivations.\textsuperscript{279} This is particularly true where the rights at stake are as fundamental as those at stake here, and where the criminal justice system will be harmed rather than helped by widespread enforcement of enemy combatant threat bargains.\textsuperscript{280} Thus, because they arise from an environment that improperly chills the defendant’s exercise of the Sixth Amendment right to a jury trial, courts should hold enemy combatant threat bargains per se unenforceable as a violation of the defendant’s Fifth Amendment right to due process.\textsuperscript{281} In time, such a ruling would have the salutary effect of constraining the influence of enemy combatant detention on the criminal justice system, both by deterring prosecutors from offering such bargains and by encouraging executive or legislative constraints on the enemy combatant detention power.\textsuperscript{282}

\textsuperscript{277} See id.
\textsuperscript{279} See id. at 28–29.
\textsuperscript{280} See id.
\textsuperscript{281} See id. at 27–29; \textit{Pearce}, 395 U.S. at 723–24; \textit{Jackson}, 390 U.S. at 583–85.
\textsuperscript{282} Cf. \textit{Miranda v. Arizona}, 384 U.S. 436, 490 (1966) (suggesting a particular warning to safeguard defendants’ rights during custodial interrogations but indicating that Congress and the states are free to develop their own safeguards so long as they are equally effective). One possible legislative solution would be for Congress to make clear that it has not authorized the enemy combatant power in any instance outside the context of battlefield captures. \textit{See Hamdi}, 542 U.S. at 518 (holding that the AUMF authorizes the detention of Hamdi, who was captured on an Afghan battlefield, as a fundamental incident of war); \textit{Padilla I}, 542 U.S. at 464 (Stevens, J., dissenting) (arguing that the AUMF does not authorize the long-term incommunicado detention of U.S. citizens arrested in the United States). Another, less dramatic solution would be to prohibit the Defense Department, through legislation or an inter-agency agreement, from designating a person as an enemy combatant after that person has been indicted pursuant to a federal terrorism investigation. \textit{See} \textit{Radack}, \textit{supra} note 6, at 542 (criticizing the absence of such restrictions). Even if the political branches failed to take action, however, courts sitting in equity could achieve a similar result by putting the government to an election of remedies: that is, forcing the government to choose between enemy combatant detention and criminal prosecution soon after the defendant’s arrest. \textit{See} United States v. Or. Lumber Co., 260 U.S. 290, 294–99 (1922) (describing election of remedies as an equitable doctrine barring a party, after
Conclusion

Plea bargaining is an important part of our judicial system. For two major reasons, however, plea bargains induced by threats of enemy combatant detention should not be governed by normal plea bargaining standards. First, enemy combatant threat bargains do not arise from the normal give-and-take of plea bargaining, because the choice between a plea bargain and extrajudicial enemy combatant detention—with its limited due process guarantees, stark differences from a criminal trial, and unrelatedness to criminal justice objectives—creates an extraordinary pressure to plead guilty unlike that of any normal plea bargaining tactic. Second, enemy combatant threat bargains create serious public policy concerns and serve few societal interests, because they lack the mutuality of benefits that characterizes normal plea bargains, substantially increase the chance that innocent defendants will plead guilty, serve no societal interests that could not be served equally well by other means, and threaten both the integrity of the criminal justice system and the rule of law. Because enemy combatant threat bargains chill defendants’ exercise of their Sixth Amendment right to a jury trial and do not deserve the deference courts normally afford normal plea bargains, and because the limited factual basis required for an enemy combatant designation will starve for facts any case-by-case balancing of interests, the most appropriate judicial response is to hold enemy combatant threat bargains per se unenforceable under the Due Process Clause of the Fifth Amendment.

Carl Takei
CONFIDENTIAL INFORMANTS IN NATIONAL SECURITY INVESTIGATIONS

Abstract: Although a body of law has developed around the use of confidential informants in criminal investigations, the role of informants in national security matters is less clearly defined. This Note first examines the limitations on the use of informants in the criminal context that are imposed by the Fourth Amendment, a detailed set of guidelines issued by the Attorney General, and other sources of law. It then turns to the treatment of informants by the major sources of national security law, including the Foreign Intelligence Surveillance Act. Ultimately, this Note concludes that in the national security context, government agents are free from many of the restrictions placed on the use of informants in criminal investigations. Although this relative freedom may be necessary given the immediate challenge of combating international terrorism, care should be taken that the executive branch does not use informants in a way that violates individual privacy or oversteps other proper investigative boundaries.

Introduction

Informants, otherwise known as “snitches” or “rats,” are people who report to the authorities on the criminal activity of others.¹ Informants may be one-time providers of information or recurring agents of law enforcement.² By nature, many informants are criminals themselves, and, as a result, law enforcement agents in the United States often rely on criminals to help solve and prevent crimes.³ As a practical reality, informants are a necessary evil in criminal investigations, but employing underworld figures as allies may create legal and ethi-

¹ See Robert M. Bloom, Ratting: The Use and Abuse of Informants in the American Justice System 1–7 (2002) (introducing the role of informants throughout history); Dick Lehr & Gerard O’Neill, Black Mass: The Irish Mob, the FBI, and a Devil’s Deal, at xiii (2000) (referring to informants as “snitch[es]” and “rats”).
² Bloom, supra note 1, at 1.
³ See id. at 1–7.
cal concerns. Therefore, a body of law has developed around the use of informants in criminal investigations.

The nation’s law-enforcement agencies now face a major new challenge: preventing another terrorist attack inside the United States. As some reports suggest, the Federal Bureau of Investigation (the “FBI”) and other agencies have engaged informants with links to terrorist organizations in order to detect and prevent future terrorist plots. In national security investigations, however, the policies regarding informants differ from those in the criminal context. This Note addresses how the rules governing the use of informants change when national security is at stake.

The law imposes a number of restrictions on the use of informants in criminal investigations. Under the Fourth Amendment, courts may issue search warrants on the basis of information provided by an informant, but only upon a preliminary demonstration that the source of such information is somewhat reliable. An even more stringent standard of review is imposed upon the use of informants to support an application for electronic surveillance. In addition to these warrant requirements, other defenses and remedies exist for the criminally accused whose rights may have been violated during an investigation involving the use of informants. Furthermore, the Attorney General has issued detailed guidelines regulating the manner in

---

4 For a discussion of the legal and ethical problems attending the use of informants in the criminal context, see infra notes 28–104 and accompanying text.
8 See infra notes 105–212 and accompanying text.
9 See infra notes 28–56 and accompanying text.
10 See infra notes 50–56 and accompanying text.
11 See infra notes 57–72 and accompanying text.
which federal agents should handle confidential informants in criminal investigations.\textsuperscript{12}

When conducting national security investigations, however, federal agents have broader discretion regarding the use of informants.\textsuperscript{13} A 1981 Executive Order grants authority to the FBI and other agencies to collect domestic national security intelligence when the target of the investigation is an agent of a foreign power.\textsuperscript{14} Furthermore, an act of Congress—the Foreign Intelligence Surveillance Act of 1978 (“FISA”)—sets forth procedures for investigating an agent of a foreign power that depart from the requirements of a criminal search or surveillance warrant.\textsuperscript{15} Under these provisions, federal agents may initiate electronic surveillance or even physical searches without following ordinary warrant procedures, and as a result, courts are less involved in supervising the use of informants.\textsuperscript{16} Additionally, new guidelines from the Attorney General relating to national security investigations effectively remove the restrictions placed on federal agents when it comes to handling informants.\textsuperscript{17}

Part I of this Note introduces the body of law governing the use of informants in criminal investigations.\textsuperscript{18} Part II discusses the role of informants in the context of national security and examines the differences between the two bodies of law.\textsuperscript{19} In national security matters, if the target of an investigation can be classified as an agent of a foreign power, the range of investigative techniques available to the FBI and other agencies is much more extensive than in criminal investigations.\textsuperscript{20} Furthermore, the legal protections available to criminal defendants become irrelevant if no criminal prosecution results from an intelligence investigation.\textsuperscript{21} Part III considers whether these differences are appropriate, in light of concerns about concentrated execu-

\begin{footnotes}
\item[12]See infra notes 73–104 and accompanying text.
\item[13]See infra notes 105–212 and accompanying text.
\item[16]See infra notes 105–175 and accompanying text.
\item[17]See infra notes 176–212 and accompanying text.
\item[18]See infra notes 24–104 and accompanying text.
\item[19]See infra notes 105–212 and accompanying text.
\item[20]See infra notes 105–212 and accompanying text.
\item[21]See infra notes 105–212 and accompanying text.
\end{footnotes}
tive power and infringement upon individual privacy.\textsuperscript{22} Although these policies reflect a legitimate, elevated fear of the threat from foreign terrorism, they also open the door to increased and largely unsupervised use of confidential informants acting as spies within the United States.\textsuperscript{23}

\section*{I. Informants in the Criminal Context}

The U.S. Constitution provides criminal defendants with certain protections regarding information provided by confidential informants.\textsuperscript{24} Guidelines issued by the Attorney General also limit the ways in which confidential informants may be utilized in criminal investigations.\textsuperscript{25} This Part discusses the standard of review for information provided by informants that is used to support a search warrant or an application for electronic surveillance, in addition to other constitutional protections associated with the use of informants in criminal investigations.\textsuperscript{26} It then introduces the Attorney General's guidelines on the use of confidential informants.\textsuperscript{27}

\textbf{A. Search Warrants and Applications for Electronic Surveillance}

The Fourth Amendment states that search warrants shall issue only upon a showing of “probable cause.”\textsuperscript{28} A judge or other magistrate must review an application for a search warrant and determine that there is probable cause to believe that evidence of a crime exists in a particular place before issuing the warrant.\textsuperscript{29} Police officers often seek to establish probable cause for a search warrant based on information provided by confidential informants.\textsuperscript{30} In a pair of cases from the 1960s—\textit{Spinelli v. United States} and \textit{Aguilar v. Texas}—the U.S. Supreme Court developed a two-prong test for determining whether information provided by a confidential informant is sufficient to establish

\textsuperscript{22} See \textit{infra} notes 213–254 and accompanying text.
\textsuperscript{23} See \textit{infra} notes 105–254 and accompanying text.
\textsuperscript{24} See \textit{infra} notes 28–72 and accompanying text.
\textsuperscript{25} See \textit{infra} notes 73–104 and accompanying text.
\textsuperscript{26} See \textit{infra} notes 28–104 and accompanying text.
\textsuperscript{27} See \textit{infra} notes 28–104 and accompanying text.
\textsuperscript{28} U.S. Const. amend. IV (“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 . . . .”); see \textit{Spinelli v. United States}, 393 U.S. 410, 416–19 (1969); \textit{Aguilar v. Texas}, 378 U.S. 108, 114 (1964).
\textsuperscript{30} Bloom, \textit{supra} note 1, at 38–39.
probable cause for a search warrant.\textsuperscript{31} One prong of the \textit{Aguilar-Spinelli} test required that the informant have an actual basis of knowledge of criminal activity, as demonstrated by a showing of specific facts.\textsuperscript{32} The other prong required a demonstration to a judge that that the informant is a credible source.\textsuperscript{33} The two-prong \textit{Aguilar-Spinelli} test was used for years, and a deficiency in either prong was enough to undermine a finding of probable cause.\textsuperscript{34}

The Court later modified this rule in the 1983 case of \textit{Illinois v. Gates} by adopting a “totality of the circumstances” approach.\textsuperscript{35} Under \textit{Gates}, the task of the magistrate issuing the warrant is to make a practical, commonsense decision as to whether probable cause exists for purposes of the Fourth Amendment, taking into account both of the \textit{Aguilar-Spinelli} factors—basis of knowledge of criminal activity and the credibility of the informant—such that a “fair probability [exists] that contraband or evidence of a crime will be found in a particular place.”\textsuperscript{36} By not requiring strict adherence to either of the \textit{Aguilar-Spinelli} prongs, this test makes it easier for the police to obtain search warrants based on information provided by confidential informants.\textsuperscript{37} Under \textit{Gates}, however, courts still are involved with evaluating the credibility of informants used to establish probable cause in a search warrant affidavit.\textsuperscript{38}

Even with the \textit{Gates} constitutional requirement, it is possible for police officers to fabricate the existence of informants in order to obtain a search warrant, because it is difficult to demonstrate that a police officer is lying in a search warrant application.\textsuperscript{39} The Supreme Court has generally held that the identity of an informant need not be disclosed in a warrant application, even where the defendant challenges the probable cause determination.\textsuperscript{40} In order to get a hearing to determine the veracity of a sworn statement in a search warrant affidavit, a defendant first must make a substantial preliminary show-

\textsuperscript{31} See \textit{Spinelli}, 393 U.S. at 416–19; \textit{Aguilar}, 378 U.S. at 114.
\textsuperscript{32} See \textit{Spinelli}, 393 U.S. at 416–19; \textit{Aguilar}, 378 U.S. at 114.
\textsuperscript{33} See \textit{Spinelli}, 393 U.S. at 416–19; \textit{Aguilar}, 378 U.S. at 114.
\textsuperscript{34} See \textit{Bloom}, supra note 1, at 39.
\textsuperscript{35} 462 U.S. at 238. The stricter \textit{Aguilar-Spinelli} test is still used in some states, including Massachusetts. See \textit{Commonwealth v. Upton}, 476 N.E.2d 548, 556–58 (Mass. 1985).
\textsuperscript{36} \textit{Gates}, 462 U.S. at 238.
\textsuperscript{37} See \textit{id.}; \textit{Spinelli}, 393 U.S. at 416–19; \textit{Aguilar}, 378 U.S. at 114.
\textsuperscript{38} See \textit{Gates}, 462 U.S. at 239 (“Sufficient information must be presented to the magistrate to allow that official to determine probable cause; his action cannot be a mere ratification of the bare conclusions of others.”).
\textsuperscript{40} See \textit{McCray v. Illinois}, 386 U.S. 300, 305 (1967).
ing that a false statement was made knowingly and intentionally, or with reckless disregard for the truth.\textsuperscript{41} This high standard makes it difficult to convince a judge of the possibility that a police officer might be lying in a warrant affidavit, and serves as an obstacle to getting a hearing to challenge the veracity of the officer’s statement.\textsuperscript{42} Although it is impossible to know exactly how often the police invent informants to obtain search warrants, evidence suggests that “testifying” does occur in the world of law enforcement.\textsuperscript{43} Nevertheless, the fact that a court must at least review a warrant application, which would include information provided by informants, still provides an independent check on law enforcement discretion.\textsuperscript{44}

In addition to physical searches of places or people, law enforcement agents also conduct electronic surveillance in criminal investigations, including methods such as wiretapping a phone or bugging a room.\textsuperscript{45} Like physical searches and seizures, electronic surveillance falls within the ambit of the Fourth Amendment protection against unreasonable searches and seizures.\textsuperscript{46} In the 1967 case of \textit{Katz v. United States}, the U.S. Supreme Court held that a warrantless listening device used in a telephone booth violated the Fourth Amendment protection against unreasonable searches.\textsuperscript{47} Famously declaring that “the Fourth Amendment protects people, not places,” the Court held that an individual has an expectation of privacy in communications made over the telephone and that therefore government agents may not employ wiretaps without a warrant supported by probable cause.\textsuperscript{48}

\begin{itemize}
\item \textsuperscript{41} \textit{Franks}, 438 U.S. at 155–56.
\item \textsuperscript{42} \textit{See id.}
\item \textsuperscript{43} \textit{Bloom}, supra note 1, at 43.
\item \textsuperscript{44} \textit{See United States v. U.S. Dist. Court (Keith), 407 U.S. 297, 317 (1972)} (“The Fourth Amendment contemplates a prior judicial judgment . . . . This judicial role accords with our basic constitutional doctrine that individual freedoms will best be preserved through a separation of powers and division of functions among the different branches and levels of Government.”) (footnote and citation omitted).
\item \textsuperscript{45} \textit{See 50 U.S.C. § 1801(f) (2000 & Supp. III 2003)} (defining electronic surveillance, for the purposes of FISA, as the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire or radio communication). Electronic surveillance may also include the use of telephonic “pen registers” and “trap and trace devices.” \textit{See 50 U.S.C. § 1841 (2000)}.
\item \textsuperscript{46} \textit{See Katz v. United States}, 389 U.S. 347, 348 (1967).
\item \textsuperscript{47} \textit{Id.} at 359.
\item \textsuperscript{48} \textit{Id.} at 351, 359.
\end{itemize}
itly left open the question of whether warrantless wiretapping would be permitted in situations involving national security.\footnote{Id. at 358 n.23 (“Whether safeguards other than prior authorization by a magistrate would satisfy the Fourth Amendment in a situation involving the national security is a question not presented in this case.”).}

B. Other Protections and Defenses

Other constitutional amendments also offer some protection to criminal defendants when the prosecution’s case is built on evidence obtained from informants. The Sixth Amendment provides protection to the accused once judicial proceedings have commenced.\(^{57}\) In the 1964 case of *Massiah v. United States*, the Supreme Court held that the government may not use an informant as an agent to deliberately elicit statements from a suspect after the initiation of judicial proceedings—the point at which the Sixth Amendment right to counsel attaches.\(^{58}\) The Supreme Court affirmed the *Massiah* doctrine in the 1980 case of *United States v. Henry*, holding that the government may not deliberately employ jailhouse informants to initiate conversations with other inmates and thereby encourage incriminating statements.\(^{59}\) The Sixth Amendment is not violated, however, if a jailhouse informant is merely a passive listener who reports on the incriminating statements of other inmates, but does nothing to elicit those statements intentionally.\(^{60}\)

The Due Process Clause of the Fourteenth Amendment also protects defendants from the use of certain statements made to informants.\(^{61}\) Under the “voluntariness” standard, due process requires that the police not use oppressive or coercive conduct to obtain statements from criminal suspects.\(^{62}\) The Court has applied the Fourteenth Amendment voluntariness standard to the context of informants acting as government agents, holding that statements made to an informant may be suppressed if the informant is working as an agent of the government and if the statements are coerced by the informant in the scope of that agency.\(^{63}\)

\(^{57}\) *See* U.S. Const. amend. VI (“In all criminal prosecutions, the accused shall enjoy the right . . . to have the Assistance of Counsel for his defence.”).

\(^{58}\) 377 U.S. 201, 205–06 (1964).


\(^{60}\) *See* Kuhlmann v. Wilson, 477 U.S. 436, 459 (1986).

\(^{61}\) *See* U.S. Const. amend. XIV; Colorado v. Connelly, 479 U.S. 157, 164 (1986).

\(^{62}\) *See* Connelly, 479 U.S. at 164. Although the Due Process Clause of the Fourteenth Amendment applies only to state action, the voluntariness inquiry is the same under the Due Process Clause of the Fifth Amendment, which applies to the federal government. *E.g.*, Lam v. Kelchner, 304 F.3d 256, 264 (3d Cir. 2002).

\(^{63}\) *See* Arizona v. Fulminante, 499 U.S. 279, 287 (1991). The Court has also held, however, that the harmless error standard applies to such statements—a standard that makes it less likely that convictions will be reversed when partially based upon coerced incriminating statements made to informants. *See id.* at 295.
Finally, other defenses may be available to criminal defendants when informants are involved, including the doctrines of entrapment and outrageous government conduct.\textsuperscript{64} While not constitutional in origin, these defenses may be invoked under exceptional circumstances to dispose of an indictment altogether.\textsuperscript{65} In the 1992 case of \textit{Jacobson v. United States}, the Supreme Court held that “[g]overnment agents may not originate a criminal design, implant in an innocent person’s mind the disposition to commit a criminal act, and then induce commission of the crime so that the Government may prosecute.”\textsuperscript{66} Thus, a criminal defendant may raise a defense of entrapment where an informant, working as a government agent, actually induces the defendant to commit a crime and where that defendant otherwise lacked the predisposition to commit that crime.\textsuperscript{67}

A related defense is outrageous government conduct, which is similar to the defense of entrapment except that it focuses on the conduct of the government rather than on the predisposition of the defendant.\textsuperscript{68} Presumably, there may be circumstances where an informant, acting as a government agent, engages in conduct that is so outrageous during the course of an investigation that it warrants the dismissal of the indictment.\textsuperscript{69} The Second Circuit has expressed reluctance to dismiss indictments based on this defense, however, concluding that it is the province of the executive branch to determine the appropriate bounds of conduct for its investigative agents, including informants.\textsuperscript{70}

Alternatively, an individual who is not accused of a crime, but whose rights have been violated by the use of informants, may also seek civil damages from the government. In the 1971 case of \textit{Bivens v. Six Unknown Named Agents of Federal Bureau of Narcotics}, the Supreme Court held that individuals may sue federal agents for money damages arising from violations of their constitutional rights that occur during the course of an investigation, even when no criminal prosecution results.\textsuperscript{71} The \textit{Bivens} doctrine is the common-law analog to 42

\textsuperscript{64} See Schreiber, \textit{supra} note 5, at 344–49.
\textsuperscript{65} See \textit{id}.
\textsuperscript{67} See \textit{id}. at 548–51.
\textsuperscript{68} See United States v. Russell, 411 U.S. 423, 431 (1973). In \textit{United States v. Russell}, the Court suggested that there may be circumstances where the government’s investigatory conduct is so outrageous that dismissal of an indictment may be warranted on due process grounds. \textit{Id}.
\textsuperscript{69} See \textit{id}.
\textsuperscript{70} See United States v. DeSapio, 435 F.2d 272, 281–82 (2d Cir. 1970).
\textsuperscript{71} See 403 U.S. 388, 397 (1971).
U.S.C. § 1983, which creates a statutory right for individuals to sue state and local government actors for civil rights violations.\(^{72}\)

C. “Top Echelon” and the Attorney General’s Informant Guidelines

Although the safeguards discussed above exist to protect the rights of individuals from the unscrupulous use of informants by the government, law enforcement agencies, particularly the FBI, exercise significant discretion regarding the use of informants.\(^{73}\) In order to combat organized crime (once the top priority of the Bureau), the FBI developed a highly secretive, effective, and potentially dangerous system for gathering intelligence through informants—the Top Echelon Informant Program.\(^{74}\) In the FBI vernacular, Top Echelon (“TE”) informants are those who are directly involved with high levels of organized crime and are therefore serious criminals themselves.\(^{75}\)

The TE Informant Program has its roots in the 1950s, when the FBI began to shift its focus from investigating communism to fighting the Mafia.\(^{76}\) In order to gather quality information on the mob, the FBI needed informants, but informants were rare in the Mafia world because members of the organization took oaths requiring them to kill anyone among them who provided information to law enforcement.\(^{77}\) As a result, the FBI launched the ambitious TE Informant Program, which sought to recruit active, ranking members of the Mafia as informants, with the government guaranteeing absolute confidentiality regarding their identities in exchange for information.\(^{78}\)

The TE program existed almost entirely in secrecy until criminal proceedings in Boston in the late 1990s revealed its sordid details.\(^{79}\) The ethical and legal challenges facing the FBI in choosing to associate


\(^{73}\) See infra notes 74–104 and accompanying text.

\(^{74}\) See Ralph Ranalli, *Deadly Alliance: The FBI’s Secret Partnership with the Mob* 56–60 (2001).

\(^{75}\) See id. at 57.

\(^{76}\) Id. at 48–49.

\(^{77}\) United States v. Salemme, 91 F. Supp. 2d 141, 287 (D. Mass. 1999) (“Each took an oath swearing, among other things, that he would abide by ‘omerta,’ the code of silence. On at least two occasions, the inductee promised to kill without hesitation any police informant posing a threat to the Family, even if the informant were his son or brother.”), rev’d in part sub nom. United States v. Flemmi, 225 F.3d 78 (1st Cir. 2000); Ranalli, supra note 74, at 55.

\(^{78}\) Ranalli, supra note 74, at 57–59.

\(^{79}\) See infra notes 80–85 and accompanying text.
with criminals came to light at that time when Massachusetts District Court Judge Mark L. Wolf conducted a lengthy set of pretrial hearings in the case of United States v. Salemme, thereby uncovering the extensive relationship between the FBI and its informants in the Boston area. According to the court’s findings, two of Boston’s most notorious organized crime figures, James “Whitey” Bulger and Stephen “The Rifleman” Flemmi, had been acting as TE informants for the FBI for decades. Bulger and Flemmi provided information on the criminal organization La Cosa Nostra (the “LCN”) in exchange for the FBI’s sanction of their own loan-sharking and gambling activities. Thus, while their own criminal enterprise (known as the Winter Hill Organization) flourished, Bulger and Flemmi supplied valuable information to the FBI, effectively wiping out their rivals in the LCN. The court’s findings uncovered a scandal that resulted in the conviction of FBI agent John Connolly for protecting Bulger and Flemmi, his valued informants, and for tipping off Bulger to his eventual indictment. Flemmi reached a plea agreement for his cooperation in other cases, and Bulger is still a fugitive, currently on the FBI’s Top Ten Most Wanted List.

In response to the Boston scandal, Attorney General Janet Reno issued, in January of 2001, a document titled, “Guidelines Regarding the Use of Confidential Informants.” Older versions of informant guidelines had existed in some form since 1976, when they were implemented in an attempt to reform the FBI’s investigative techniques in light of revelations of abuses of power by the Bureau. The Reno review of the guidelines was spurred in large part by evidence of the FBI’s mishandling of Bulger and Flemmi, and the resulting guidelines

---

80 See 91 F. Supp. 2d at 175–316. For further discussion of the legal implications of Salemme, see Bloom, supra note 1, at 81–105; Schreiber, supra note 5, at 330–41.
81 Salemme, 91 F. Supp. 2d at 148–49. For detailed accounts of the Bulger/Flemmi affair, see generally Lehr & O’Neill, supra note 1, and Ranalli, supra note 74.
82 Salemme, 91 F. Supp. 2d at 151–57.
83 Id. at 149–57.
84 See United States v. Connolly, 341 F.3d 16, 19 (1st Cir. 2003).
87 See OIG COMPLIANCE REPORT, supra note 7, at 36–59.
were an attempt to correct those mistakes. The guidelines were reissued by former Attorney General John Ashcroft in 2002 in substantially similar form to the Reno version (the “Informant Guidelines”); this newer version remains in effect today.

The current Informant Guidelines are applicable to all domestic investigations conducted by agencies within the Department of Justice, including the FBI. The Guidelines are designed to control the relationship between informants and their government handlers; they establish standards governing the suitability of informants and require a higher-ranking FBI official than the case agent to review annually each informant’s file. Additionally, they establish a Confidential Informant Review Committee within the FBI to assess periodically the ongoing suitability of registered informants. The Guidelines specifically state that the FBI may not withhold the identity of its informants if the information is requested by any federal prosecutor’s office. Furthermore, the Guidelines describe in detail the kind of behavior that is prohibited between an informant and a federal agent, including a ban on the exchange of gifts or other monetary payments without specific approval.

Another major restriction imposed by the Informant Guidelines concerns immunity. The Informant Guidelines state that federal law enforcement agents may not immunize informants from prosecution for specific crimes, nor authorize the commission of certain future crimes, in exchange for information—at least, not without prior approval of an official within the Department of Justice. Furthermore, the Guidelines prevent agents from making, without prior written approval from a U.S. Attorney’s office, “any promise or commitment . . .

---

88 See id.
90 See infra notes 180–197 and accompanying text.
91 Informant Guidelines, supra note 89, at 9.
92 Id. at 5, 10. Once an individual has been deemed suitable to be a confidential informant, that person is “registered” as such, and certain records on that informant must be kept on file. Id. at 11.
93 Id. at 5.
94 Id. at 17.
95 Id. at 5, 19–24.
96 Informant Guidelines, supra note 89, at 5, 19–24.
that would limit the use of any evidence by the government” against the informant.97

These prohibitions in the Informant Guidelines reflect a ruling by the First Circuit in United States v. Flemmi regarding “use immunity,” or immunity with respect to the fruits of electronic surveillance.98 The court held that when an informant offers evidence to support a Title III application, an individual FBI agent does not have the authority to immunize that informant as to any incriminating statements that might later be intercepted in the course of the resulting surveillance.99 An agent may promise to keep the identity of the informant confidential, but he or she may not grant any form of immunity without seeking further authorization from an official within the Department of Justice.100 The Informant Guidelines essentially incorporate this holding.101

A recent review of the FBI’s compliance with the Guidelines, conducted by the Office of the Inspector General (the “OIG”) and detailed in a report issued in September 2005, found that the Bureau has not adequately supported or implemented the Informant Guidelines.102 The OIG’s comprehensive compliance report noted that the FBI is in the process of considering significant changes to its informant program, and it made several specific recommendations for properly implementing the Informant Guidelines.103 The report’s findings also indicated the ongoing importance of informants to FBI investigations, as well as the necessity of maintaining and improving procedures for proper oversight of criminal informants.104

II. INFORMANTS IN THE NATIONAL SECURITY CONTEXT

As discussed in Part I, there are limits on how law enforcement agents may use informants in criminal investigations.105 When the nature of an investigation involves a threat to national security, however, differ-
ent rules apply. Courts have granted the executive branch broad discretion over national security matters. The Supreme Court has left open the issue of whether the Fourth Amendment applies in national security investigations, and several circuit courts of appeals have held that it does not. Consequently, in the field of national security, federal investigative agencies are governed by three alternative sources of authority: a 1981 executive order issued by President Reagan, a congressional act from 1978, and guidelines issued by the Attorney General. This Part discusses the role of informants in national security investigations, as construed from these sources of authority.

A. Executive Order No. 12,333 and Intelligence Investigations

The President has the fundamental duty to “preserve, protect and defend the Constitution of the United States.” From this executive duty flows the power of executive agencies to investigate and ultimately defend the country from foreign threats. When national security is at stake, courts have granted the federal government’s executive branch the authority to act outside the scope of the Fourth Amendment. The Supreme Court addressed the scope of the executive power to conduct warrantless searches in national security investigations in 1972.
in *United States v. U.S. District Court (Keith).*\(^{117}\) In *Keith,* the Court held that federal law enforcement agents must seek warrants for searches when the target of the investigation is purely “domestic,” even when the investigation implicates national security concerns.\(^{118}\) The ruling at the time applied to both physical searches and electronic surveillance.\(^{119}\) However, the *Keith* Court specifically left open the issue of the existence of executive power to conduct warrantless searches or surveillance with respect to the activities of “foreign powers or their agents.”\(^{120}\) Consequently, it has been left to the U.S. circuit courts of appeals to recognize a limited national security exception to the Fourth Amendment warrant requirement; four courts have done so, although the Supreme Court has not explicitly approved this view.\(^{121}\)

In 1981, President Reagan issued Executive Order No. 12,333, thereby claiming for the executive branch the power to conduct warrantless searches and surveillance of agents of a foreign power.\(^{122}\) Within the executive branch, the FBI is the entity primarily responsible for gathering domestic national security intelligence.\(^{123}\) The Executive Order places the FBI in charge of gathering intelligence within the United States, leaving the Central Intelligence Agency (the “CIA”) responsible for gathering intelligence abroad.\(^{124}\) The FBI thus functions not only as a federal police force, but also as a domestic spy agency.\(^{125}\) The Bureau maintains an Office of Intelligence that shares information with other intelligence agencies throughout the federal government.\(^{126}\) Other entities within the “intelligence community” of

---


\(^{118}\) 407 U.S. at 321.

\(^{119}\) See id.

\(^{120}\) Id.


\(^{123}\) Id. § 1.14(a), 3 C.F.R. at 210, *reprinted in* 50 U.S.C. § 401 note.


\(^{125}\) See Mueller, *supra* note 6, at 120.

\(^{126}\) Id.
the executive branch include the Department of State, the Department of Defense, and the National Security Agency.\footnote{127}{Exec. Order No. 12,333, §§ 1.4–1.14, 3 C.F.R. at 202–10, \textit{reprinted in} 50 U.S.C. § 401 note.}

Executive Order No. 12,333 grants the Attorney General the power to authorize investigative techniques that otherwise would require a warrant if the Attorney General determines in each case that there is probable cause to believe that the “technique” is directed against a foreign power or an agent of a foreign power.\footnote{128}{\textit{Id.} § 2.5, 3 C.F.R. at 212, \textit{reprinted in} 50 U.S.C. § 401 note (2000). For a discussion of the term “agent of a foreign power” as defined by FISA, see \textit{infra} notes 147–151 and accompanying text.} The Order does not define the term “technique,” although it states that “[e]lectronic surveillance, as defined in the Foreign Intelligence Surveillance Act of 1978, shall be conducted in accordance with that Act, as well as this Order.”\footnote{129}{Exec. Order No. 12,333, § 2.5, 3 C.F.R. 200, 212 (1982), \textit{reprinted in} 50 U.S.C. § 401 note.} Because the language only qualifies the term “technique” by stating that electronic surveillance must be conducted in accordance with FISA, an inference may be drawn that the word “technique” includes electronic surveillance as well as other investigative practices, such as traditional physical searches.\footnote{130}{See \textit{id.}, \textit{reprinted in} 50 U.S.C. § 401 note.} “Foreign intelligence” is defined as “information relating to the capabilities, intentions and activities of foreign powers, organizations or persons.”\footnote{131}{See \textit{id.} § 3.4(d), 3 C.F.R. at 215, \textit{reprinted in} 50 U.S.C. § 401 note.} These provisions therefore authorize the FBI, at the direction of the Attorney General, to circumvent the warrant requirement when national security is at risk from a foreign threat.\footnote{132}{See \textit{Exec. Order No. 12,333, § 2.5, 3 C.F.R. at 212, \textit{reprinted in} 50 U.S.C. § 401 note.} Such searches must be undertaken for intelligence purposes only, not “law enforcement” purposes—meaning that evidence collected without a warrant would still not be admissible in a criminal prosecution.\footnote{133}{See \textit{Keith}, 407 U.S. at 318–24; \textit{Exec. Order No. 12,333, § 2.5, 3 C.F.R. at 212, \textit{reprinted in} 50 U.S.C. § 401 note.}

The Executive Order makes no explicit reference to the use of confidential informants, but by eliminating the warrant requirement, it authorizes federal agents to conduct searches based on uncorroborated information from informants, without any concern for satisfying the \textit{Illinois v. Gates} standards for informant use in criminal investigations.\footnote{134}{See 462 U.S. 213, 238 (1983); \textit{Exec. Order No. 12,333, 3 C.F.R. 200, \textit{reprinted in} 50 U.S.C. § 401 note (2000); \textit{supra} notes 28–38 and accompanying text.} Therefore, under the provisions of Executive Order No. 12,333, intelli-
gence agencies could act on any information received from informants that they deem credible, without having to demonstrate to an independent court that the informant is reliable or has specific knowledge indicating that terrorist actions are afoot.\(^{135}\)

**B. The Foreign Intelligence Surveillance Act of 1978**

The Keith Court held that the Fourth Amendment warrant requirement does apply in domestic national security investigations.\(^{136}\) The case left open, however, the constitutionality of warrantless surveillance of foreign organizations or individuals in national security investigations.\(^{137}\) Although circuit courts of appeals have subsequently recognized an exception to the Fourth Amendment warrant requirement in national security investigations, the precise scope of executive authority in such cases has not been defined by the Supreme Court or the circuits.\(^{138}\) In the 1952 Supreme Court case *Youngstown Sheet & Tube Co. v. Sawyer* (*Steel Seizure*), Justice Jackson expressed the classic articulation of the inherent power of the executive and its relationship to congressional authority.\(^{139}\) Where the President acts pursuant to an “express or implied authorization of Congress,” Jackson wrote, “his authority is at its maximum, for it includes all that he possesses in his own right plus all that Congress can delegate.”\(^{140}\) Although there may be a “zone of twilight” where Congress and the executive branch have concurrent authority, once Congress expresses its will on a subject, the President is bound by the legislative action.\(^{141}\) As to the executive branch’s power to conduct electronic surveillance and other forms of searches in national security investigations—a “zone of twilight” of concurrent presidential and congressional authority—Congress expressed its will in the Foreign Intelligence Surveillance Act of 1978.\(^{142}\)

Enacted partially as a response to the Keith decision, FISA was designed to provide procedures for obtaining prior judicial approval of

---


\(^{136}\) 407 U.S. at 320–21.

\(^{137}\) See id. at 321–22; see also Eggert, supra note 117, at 623.

\(^{138}\) See supra notes 118–121 and accompanying text.

\(^{139}\) 343 U.S. 579, 634–55 (1952) (Jackson, J., concurring).

\(^{140}\) Id. at 635.

\(^{141}\) See id. at 637.

electronic surveillance in national security matters.\textsuperscript{143} In ordinary criminal investigations, Title III court orders must be obtained from a federal district court in order to perform electronic surveillance.\textsuperscript{144} But Title III did not address the issue of whether warrants for electronic surveillance are required in national security cases.\textsuperscript{145} FISA created the Foreign Intelligence Surveillance Court (the “FISC”), a special court that operates in secret, to issue warrants for electronic surveillance in national security matters.\textsuperscript{146} Federal agents may apply directly to the FISC for authorization to conduct electronic surveillance against an “agent of a foreign power” without having to make an application in open federal district court.\textsuperscript{147} FISA defines an “[a]gent foreign power” as any person who “engages in clandestine intelligence activities in the United States contrary to the interests of the United States” on behalf of a foreign power.\textsuperscript{148} The term “agent of a foreign power” is also used in Executive Order No. 12,333, but it is not defined there; because the terms of the Order itself require adherence with FISA, the Order’s definition of this term is evidently the same as that in FISA.\textsuperscript{149} An FISC judge may issue an order for electronic surveillance upon finding probable cause that the target is an agent of a foreign power.\textsuperscript{150} Be-

\textsuperscript{143} See Eggert, \textit{supra} note 117, at 638.

\textsuperscript{144} See 18 U.S.C. § 1518 (2000); \textit{supra} notes 50–56 and accompanying text.

\textsuperscript{145} \textit{See supra} notes 50–56 and accompanying text.

\textsuperscript{146} 50 U.S.C. § 1803(a) (2000 & Supp. III 2003); \textit{see In re Sealed Case}, 310 F.3d at 719.


\textsuperscript{148} 50 U.S.C. § 1801(b); \textit{see supra} note 147 and accompanying text.


\textsuperscript{150} 50 U.S.C. § 1805(a). If the target of the surveillance is a U.S. citizen or otherwise a legal resident of the United States, then there must be probable cause to believe that the target’s activities involve espionage or other similar conduct in violation of the criminal statutes of the United States, and the surveillance application must not rely solely upon the basis of speech, association, and other activities protected by the First Amendment. \textit{Id.}
cause an agent of a foreign power is defined as someone “other than a United States person” operating “in the United States,” FISA is not concerned with surveillance conducted against aliens in foreign lands.\textsuperscript{151}

Because Congress has specifically granted the executive limited powers to conduct electronic surveillance and even physical searches without a warrant within the United States in national security investigations through FISA, there is a presumption, under Justice Jackson’s formula in \textit{Steel Seizure}, that such conduct is constitutional.\textsuperscript{152} Indeed, the electronic surveillance provisions of FISA have been upheld as constitutional by the Second Circuit Court of Appeals.\textsuperscript{153} And although the Supreme Court has never explicitly upheld warrantless physical searches in national security cases, the Fourth Circuit has recognized a general national security exception to the warrant requirement for conducting foreign intelligence surveillance—meaning that such surveillance lies outside the scope of the Fourth Amendment.\textsuperscript{154} Therefore, FISA, and not Fourth Amendment caselaw, provides the primary external check on the investigatory methods of the executive branch in national security matters.\textsuperscript{155}

\section*{C. FISA Mechanics and Informants}

Although FISA requires prior judicial approval of electronic surveillance in foreign intelligence investigations in most instances, warrantless surveillance may be authorized directly by the Attorney General if certain procedures are followed.\textsuperscript{156} Under § 1802(a), the Attorney General may authorize warrantless electronic surveillance for up to one year if it is directed solely against a foreign power and there is

\begin{footnotesize}
\begin{itemize}
\item \textsuperscript{151} 50 U.S.C. § 1801(b) (emphasis added); see supra note 147 and accompanying text; see also United States v. Verdugo-Urquidez, 494 U.S. 259, 271–72 (1990) (holding that the protections of the Fourth Amendment do not extend to non-citizens in foreign lands lacking “substantial connection” with the United States). By contrast, the Court held in \textit{United States v. Verdugo-Urquidez} that once an alien lawfully enters and resides in this country, he or she becomes invested with the rights guaranteed by the Constitution, including the full protections of the Fourth Amendment. 494 U.S. at 271–72. What \textit{Verdugo-Urquidez} leaves ambiguous is what constitutes a “substantial connection” for illegal aliens inside or outside the territorial jurisdiction of the United States. \textit{See id.}
\item \textsuperscript{152} \textit{See Steel Seizure}, 343 U.S. at 634–37 (Jackson, J., concurring); \textit{supra} notes 136–151 and accompanying text.
\item \textsuperscript{153} \textit{See United States v. Duggan}, 743 F.2d 59, 71–76 (2d Cir. 1984).
\item \textsuperscript{154} \textit{See Truong Dinh Hung}, 629 F.2d at 914–16.
\item \textsuperscript{155} \textit{See supra} notes 136–154 and accompanying text.
\item \textsuperscript{156} \textit{See} 50 U.S.C.A. § 1802(a) (West 2001 & Supp. 2005).
\end{itemize}
\end{footnotesize}
no substantial likelihood that communications of a U.S. person will be intercepted.157 The Attorney General is required, however, to provide certification of such action to the FISC immediately after ordering the surveillance.158 FISA also provides the Attorney General with “emergency” power to initiate electronic surveillance without prior judicial approval under § 1805 if an application is made to the FISC within seventy-two hours of the initiation of surveillance.159 Although these provisions act as a limitation on the kinds of monitoring that federal agents may conduct, they do allow for some degree of warrantless surveillance.160

Under FISA, law enforcement may also perform physical searches without a warrant under certain circumstances.161 As amended in 1994, FISA grants the Attorney General the power to authorize warrantless physical searches for up to one year to acquire foreign intelligence information, where the search is directed solely at property in the open and exclusive control of a foreign power and there is no substantial likelihood that a U.S. person will be targeted in the search.162 Just as with electronic surveillance, the Attorney General must submit certification of warrantless physical searches to the FISC immediately after they occur.163 Federal agents also may apply for FISA warrants for physical searches, just as they may apply for electronic surveillance warrants.164

Like Executive Order No. 12,333, FISA does not specifically refer to the use of confidential informants.165 In ordinary search warrants and Title III applications, informants are frequently cited as sources of information to establish probable cause.166 Presumably, then, information provided by confidential informants is likewise used to obtain FISA warrants.167 Unlike in the ordinary warrant and Title III application context, however, the precise standard applied by the FISC to informant qualification is not known because the court operates in

158 Id. § 1802(a)(3).
160 See supra notes 156–159 and accompanying text.
162 Id. §§ 1822, 1823(a).
163 Id. §§ 1802(a)(3), 1821(4)(D), 1822(a)(1).
164 See id. §§ 1823–1824.
166 See supra notes 28–56 and accompanying text.
167 See supra notes 28–56 and accompanying text.
Moreover, since FISA was enacted, only one case has been appealed to the special Foreign Intelligence Surveillance Court of Review, resulting in just one published opinion, and this opinion did not address informants. However, an internal FBI guidance memo shows that the FBI has adopted a “totality-of-the-circumstances” approach as its standard for informant qualification in FISA applications—a standard that comports with the Fourth Amendment requirement established in Gates. Although the Justice Department recommends the Aguilar-Spinelli standard for Title III applications, the FBI does not suggest this stricter standard in FISA applications. Precisely because it operates in secret, one could argue that it would make sense for the FISC to require a higher standard for informant qualification than the Gates “totality” approach, for there is no need to protect the secret identity of informants in FISA applications. On the other hand, the interest in protecting national security by allowing the surveillance favors a lower quantum of proof for securing the ability to conduct surveillance—an interest perhaps reflected in the fact that in calendar years 2003 and 2004, a combined 3485 FISA warrant applications were made, and only four were denied. But if and when the Attorney General authorizes warrantless searches or surveillance, there is no prior judicial review of the credibility of the informants providing the basis for investigative activities. In such cases,

---

168 See supra note 146 and accompanying text.
169 See In re Sealed Case, 310 F.3d at 719.
171 See Criminal Resource Manual, supra note 55, § 29(C); supra note 170 and accompanying text.
172 See Gates, 462 U.S. at 238.
174 See supra notes 156–171 and accompanying text.
federal agents are bound only by internal Department of Justice investigatory guidelines.\textsuperscript{175}

\section{D. The Attorney General’s Domestic Security Guidelines}

Former Attorney General John Ashcroft issued several sets of guidelines in 2002 and 2003 governing the investigative practices in both domestic and foreign national security investigations.\textsuperscript{176} These guidelines represent the executive branch’s internal controls over investigatory methods used by the FBI and other agencies, and they are most relevant to an agent’s day-to-day investigative authority.\textsuperscript{177} Unsurprisingly, the Bureau has a freer hand in national security investigations than in criminal investigations, particularly when the target of the investigation is an agent of a foreign power.\textsuperscript{178} These guidelines, while not legally binding, are evidence of the policy choices that the administration of President George W. Bush has made regarding the utilization of confidential informants.\textsuperscript{179}

The Informant Guidelines are not applicable to investigations of foreign intelligence, since, by their own terms, they apply only to domestic criminal investigations and prosecutions.\textsuperscript{180} They do not apply to the use of informants in foreign countries, unless the informant is reasonably likely to be called as a witness in a domestic case.\textsuperscript{181} Nor do the Informant Guidelines apply to the use of confidential informants in foreign intelligence or foreign counterintelligence investigations.\textsuperscript{182}

More recent guidelines address national security investigations specifically.\textsuperscript{183} On May 30, 2002, Ashcroft introduced an updated set of Guidelines on General Crimes, Racketeering Enterprise and Terrorism Enterprise Investigations (the “Domestic Security Guidelines”).\textsuperscript{184} The terrorism provisions in the Domestic Security Guidelines are applicable to the FBI’s investigations of groups that originate and operate inside the United States.\textsuperscript{185} The Domestic Security Guidelines state that they

\textsuperscript{175} See infra notes 176–197 and accompanying text.
\textsuperscript{176} See OIG COMPLIANCE REPORT, supra note 7, at 17, 22–23.
\textsuperscript{177} See id.
\textsuperscript{178} See infra notes 180–212 and accompanying text.
\textsuperscript{179} See supra notes 180–212 and accompanying text.
\textsuperscript{180} See INFORMANT GUIDELINES, supra note 89, at 1.
\textsuperscript{181} Id.
\textsuperscript{182} Id.
\textsuperscript{183} See infra notes 184–212 and accompanying text.
\textsuperscript{184} See generally DOMESTIC SECURITY GUIDELINES, supra note 112.
\textsuperscript{185} See id. at ii.
are not intended to supersede any applicable provisions of the Informant Guidelines.  

In criminal investigations, the Domestic Security Guidelines limit the FBI to investigating completed criminal acts or to collecting criminal intelligence information on an ongoing criminal enterprise. However, neither the Informant Guidelines nor the Domestic Security Guidelines are applicable to foreign intelligence or counterintelligence investigations, or to operations in a foreign country. Investigations of terrorist groups originating internationally but operating within the United States are covered by a separate set of guidelines. Therefore, although the Domestic Security Guidelines limit the scope of FBI investigations into criminal matters and, to a lesser extent, domestic terrorist threats, they do not limit investigations involving international terrorists.

The Domestic Security Guidelines basically preserve the Informant Guidelines in domestic criminal investigations, although they relax the conditions under which informants may be engaged. The Domestic Security Guidelines set forth the investigative procedures that may be used by FBI agents in preliminary inquiries and full investigations. Agents may begin a preliminary inquiry without even a “reasonable indication” of criminal activity when there is information or an allegation not warranting a full investigation, but still requiring further scrutiny beyond the prompt and limited checking of initial leads. The development of informants is a method available to agents at the preliminary inquiry stage. The Domestic Security Guidelines are ambiguous as to whether agents at the preliminary inquiry stage may develop new informants or only interview previously established informants. The language authorizes agents to interview “previously established informants, and other sources of information,” but the introduction to the Domestic Security Guidelines states that “[o]ther methods, including the development of sources and in-
formants” are available at the preliminary inquiry stage.196 Allowing agents at the preliminary stage not only to use established informants, but also to develop new ones, means that agents are largely unrestricted in terms of when they may seek and develop informants, although they still must act within the boundaries set forth in the Informant Guidelines.197

E. The Attorney General’s National Security Investigations Guidelines

When the target of a national security investigation is “an agent of a foreign power,” the Informant Guidelines do not apply at all, at least based on a reading of the Guidelines for FBI National Security Investigations and Foreign Intelligence Collection (the “NSI Guidelines”), introduced on October 31, 2003.198 The NSI Guidelines apply only to the FBI, and they cover investigations of foreign powers and international terrorist organizations, like Al Qaeda, operating within the United States.199 Portions of these guidelines are classified.200 The NSI Guidelines afford the FBI very broad power to investigate foreign terrorist organizations operating within the United States.201

Executive Order No. 12,333 and FISA essentially authorize the FBI to engage in domestic spying, where the targets of investigation are foreign powers or their agents.202 The NSI Guidelines reflect that authority, granting FBI agents broad power to collect foreign national security intelligence beyond what is acceptable in criminal investigations.203 The unclassified portions of the NSI Guidelines state that the “scope of authorized activities . . . is not limited to ‘investigation’ in a narrow sense, such as solving particular cases . . . . Rather, these activities also provide critical information needed for broader analytic and intelligence purposes authorized by Executive Order 12333 . . . .”204 This passage allows FBI agents to undertake broad intelligence inves-

196 Id.
197 See Domestic Security Guidelines, supra note 112, at 1, 10, 23.
198 See generally NSI Guidelines, supra note 112.
199 See id. at ii, 1–2.
200 Id. at 3–38.
201 Id. at 1–2, 11.
202 See supra notes 122–175 and accompanying text.
203 NSI Guidelines, supra note 112, at ii; see supra notes 122–175 and accompanying text (discussing Executive Order No. 12,333 and FISA). The FBI’s authority to collect intelligence in criminal investigations is outlined in the Domestic Security Guidelines. See supra notes 187–197 and accompanying text.
204 NSI Guidelines, supra note 112, at 11.
tigations, outside the bounds defined for criminal or even domestic terrorism investigations.\textsuperscript{205}

The unclassified portions of the NSI Guidelines are interesting for what they do not say: they make no reference to informants at all.\textsuperscript{206} Furthermore, the Informant Guidelines themselves state that they are not applicable to foreign intelligence or counterintelligence investigations.\textsuperscript{207} Therefore, when investigating international terrorist organizations existing or operating within the United States, it seems that the FBI is virtually unrestrained in how it may engage the assistance of informants for the purposes of investigation or intelligence-gathering.\textsuperscript{208}

Furthermore, it appears that individual agents must use their own discretion to determine whether the information they receive implicates a foreign national security threat or a domestic security threat, a decision crucial to determining which set of standards applies to the use of informants.\textsuperscript{209} Such broad discretion for FBI agents to engage informants without formal guidelines from the Department of Justice may be a necessary measure for fighting the war on terror.\textsuperscript{210} Or it may prove to concentrate too much power in the hands of the executive—a power that is subject to greater constitutional and statutory constraint in the criminal context.\textsuperscript{211} In either instance the NSI Guidelines reflect a definitive policy choice by the current administration that no rules should apply to the use of informants when foreign potential terrorists are involved.\textsuperscript{212}

\textsuperscript{205} See Domestic Security Guidelines, supra note 112, at 12, 15.
\textsuperscript{206} See generally NSI Guidelines, supra note 112.
\textsuperscript{207} Informant Guidelines, supra note 89, at 1.
\textsuperscript{208} See supra notes 198–205 and accompanying text.
\textsuperscript{209} See NSI Guidelines, supra note 112, at 2–3, 9–10; supra notes 183–197 and accompanying text.
\textsuperscript{210} See NSI Guidelines, supra note 112, at 2–3, 9–10.
\textsuperscript{211} See supra notes 28–104 and accompanying text.
\textsuperscript{212} See supra notes 198–211 and accompanying text. By contrast, the Office of the Inspector General has reiterated the importance of implementing and adhering to the Informant Guidelines in criminal and domestic security investigations. See OIG Compliance Report, supra note 7, at 133–35.
III. The Trouble with Unsupervised Use of Informants in National Security Investigations

A. Effects of Executive Order No. 12,333, FISA, and the Attorney General’s Guidelines

The combined effect of Executive Order No. 12,333, FISA, and the NSI Guidelines is that, in national security investigations under certain circumstances, the FBI and other investigative agencies currently may engage in electronic surveillance or physical searches without prior judicial approval.\textsuperscript{213} If the government does not need a warrant, it does not need to follow the informant qualification requirements of \textit{Illinois v. Gates}.\textsuperscript{214} Absent the hindrance of \textit{Gates} and prior judicial approval for a warrant, federal agents can act on the basis of any tip from any informant that they choose, without having to demonstrate to a neutral third party that the informant has a shred of credibility.\textsuperscript{215} Furthermore, unless an intelligence investigation results in a prosecution, most of the protections in place in the criminal context will never be implicated.\textsuperscript{216}

Such unilateral discretion over the use of informants by the executive branch, and unregulated discretion of individual federal agents to handle informants, raises several concerns.\textsuperscript{217} For one, agents might become too close to their most valuable informants—shielding them from prosecution to ensure their ongoing productivity, or even accepting bribes from informants and participating in their underworld activities.\textsuperscript{218} This kind of behavior was revealed in the Boston FBI scandal, when it was discovered that FBI agents had protected Whitey Bulger and Stephen Flemmi for decades because of their value as informants against the Italian Mafia.\textsuperscript{219} However, in counterterrorism investigations, this concern seems less significant than in the criminal context because it is difficult to imagine a federal agent protecting or participating in conduct that is truly threatening to national security.\textsuperscript{220}

Two other concerns merit closer consideration, however, in the sections that follow. The first concern is that using informants as a basis
for electronic surveillance without prior judicial review and approval might violate the privacy of U.S. persons. The second is that without a judicial check on the use of informants, the concentration of power in the hands of the executive branch might lead investigative agents to overstep proper boundaries. Each will be discussed in turn.

B. NSA Surveillance and Privacy Concerns

When federal agents conduct electronic surveillance or physical searches in compliance with FISA, their conduct is presumptively constitutional, and a FISC judge must at least be informed of their actions. However, reports have recently surfaced indicating that the administration of President George W. Bush has conducted warrantless electronic surveillance for years at the direction of a secret presidential order, without any sort of judicial notification or authorization. According to these reports, the National Security Agency (the “NSA”) has monitored telecommunication data regarding phone calls outside the United States that happen to pass through U.S.-based telephonic “switches.” Although this kind of surveillance is not directed at U.S. persons, it is entirely possible that the communications of U.S. citizens will be intercepted in the course of such eavesdropping. The NSA has not conducted this surveillance under the terms of FISA because federal agents desire a degree of speed and flexibility to respond to domestic terror threats that they believe FISA does not provide. The NSA surveillance program thus raises serious privacy concerns for any American using a device as technologically simple as a telephone.

---

221 See infra notes 224–254 and accompanying text.
222 See infra notes 239–254 and accompanying text.
223 See infra notes 224–254 and accompanying text.
224 See supra notes 136–175 and accompanying text.
227 See id.
228 Id.
229 See id.
Whether the executive branch has the inherent power to conduct warrantless searches or surveillance in the interest of protecting national security, beyond the scope of FISA, is debatable.\textsuperscript{230} Under Justice Jackson’s formula in \textit{Youngstown Sheet & Tube Co. v. Sawyer (Steel Seizure)}, when Congress has expressed its will on a particular matter that otherwise might exist in the “twilight” zone of concurrent executive authority, the President ought to be bound by the language of the legislation.\textsuperscript{231} Because Congress has specifically laid out procedures for conducting both electronic surveillance and physical searches under FISA, the executive should be bound to follow those rules.\textsuperscript{232} By this rationale, warrantless searches or surveillance within the United States or potentially involving U.S. persons should not take place without at least informing an independent court as to what has occurred.\textsuperscript{233}

Evidence suggests, however, that the executive branch has not consistently followed FISA, and the danger of such a practice is that it leaves an independent court completely out of the loop.\textsuperscript{234} Although the FISC authorizes the vast majority of surveillance applications, and although FISA substitutes prior authorization with subsequent notification in certain circumstances, at least with surveillance conducted pursuant to FISA, the court exercises some degree of supervision over the activity of the executive.\textsuperscript{235} This supervision does not allow federal agents to be the “sole judges of when to utilize constitutionally sensitive means in pursuing their tasks.”\textsuperscript{236} Whenever one branch of government unilaterally makes decisions affecting the privacy of individual Americans, there is the potential for abuse of discretion and misuse of information.\textsuperscript{237} To the extent that informants provide federal agents with information that can lead to unsupervised electronic surveillance by the NSA or other intelligence agencies, the executive branch may once again bypass courts and retain broad discretion in its activities, a situation that presents an undeniable threat to individual privacy.\textsuperscript{238}

\textsuperscript{230} See supra notes 136–155 and accompanying text.  
\textsuperscript{231} See 343 U.S. 579, 637 (1952) (Jackson, J., concurring).  
\textsuperscript{232} See id.  
\textsuperscript{233} See id.; supra notes 143–175 and accompanying text.  
\textsuperscript{234} See supra notes 224–229 and accompanying text.  
\textsuperscript{235} See supra notes 136–175 and accompanying text.  
\textsuperscript{237} See id.  
\textsuperscript{238} See id.
C. The Power of an Informant’s Tip

Another concern with a lack of supervision over the use of informants in investigations is that a single piece of information from an informant has the power to set off a wave of action by law enforcement officials, especially when there is a potential national security threat.\footnote{239} One such situation began on January 17, 2005, when an anonymous informant called the California Highway Patrol and told police that he had helped smuggle four Chinese nationals into the United States from Mexico.\footnote{240} According to the informant, this group was planning to launch an attack with nuclear material on the city of Boston.\footnote{241} The informant was soon apprehended, and he confessed that his claim was fictional and that he had been under the influence of drugs and alcohol at the time he made the call.\footnote{242} Officials speculated that the motivation behind the tip was vengeance; the informant, it turned out, was actually a professional human smuggler, and the four Chinese nationals were customers who failed to pay him for his services.\footnote{243} As a result of the informant’s false tip, however, law enforcement agents scrambled across the country, and a nationwide manhunt for the potential Chinese terrorists ensued.\footnote{244}

The informant’s tip in this instance did not disrupt a terrorist plot, because no such plot existed.\footnote{245} But a great deal of resources was expended and wasted, and a high degree of anxiety was caused, because of a single phone call from an intoxicated smuggler.\footnote{246} Because the tip allegedly involved foreign nationals who were supposedly involved in a terrorist threat, and because the authorities were not investigating an actual crime but were seeking intelligence to prevent a future act of terrorism, the ensuing investigation would have been governed by the broad rules set forth in Executive Order No. 12,333, FISA, and the Attorney General’s guidelines.\footnote{247} Consequently, this single tip could have led to warrantless searches across the country, as

\footnote{239}{See infra notes 240–254 and accompanying text.}
\footnote{240}{Murphy, Tipster, supra note 7, at A1.}
\footnote{241}{Id.}
\footnote{242}{Id.}
\footnote{243}{Id.}
\footnote{244}{Id.}
\footnote{245}{Murphy, Tipster, supra note 7, at A1.}
\footnote{246}{Id.}
\footnote{247}{See supra notes 122–135 and accompanying text (discussing Executive Order No. 12,333); supra notes 143–175 and accompanying text (discussing FISA); supra notes 176–212 and accompanying text (discussing the Attorney General’s guidelines).}
well as wiretaps and other forms of electronic surveillance, unilaterally approved and performed by the executive branch.248

Because the informant in this case did not seem particularly reliable, a judge or magistrate might not have issued search warrants or authorized electronic surveillance based solely on the information provided in his phone call.249 But because the tip involved an issue of national security, the emergency provisions of FISA meant that a judge was not required to approve any searches law enforcement wanted to conduct.250 Such an example raises the possibility that an individual tipster, or even prankster, could set off a wave of warrantless searches with a single phone call to the local police if that phone call happens to implicate national security concerns.251

This incident demonstrates the power that a tip from an informant has to mobilize law enforcement agencies across the country in response to a potential national security threat.252 Otherwise innocent and unsuspecting individuals may have had their homes searched or their phones tapped as a result of one phone call from a drunken smuggler.253 This incident also demonstrates why the Supreme Court has imposed rules on using informants to obtain search warrants in criminal cases: to prevent law enforcement agents from overstepping their investigatory bounds and intruding on citizens on the basis of uncorroborated or unreliable information from an informant with ulterior motives for dropping a dime.254

Conclusion

Law enforcement agents necessarily rely on information provided by unsavory informants in order to solve and prevent crimes. Over time, a set of rules has emerged governing how confidential informants should be used in criminal investigations, in the form of constitutional jurisprudence, congressional legislation, and internal Department of Justice guidelines. In the national security context, however, where the target of the investigation is an agent of a foreign power and the nature

248 See supra notes 122–135 and accompanying text (discussing Executive Order No. 12,333); supra notes 143–175 and accompanying text (discussing FISA); supra notes 176–212 and accompanying text (discussing the Attorney General’s guidelines).
249 See supra notes 28–56 and accompanying text.
251 See supra notes 239–250 and accompanying text.
252 See supra notes 122–212 and accompanying text.
253 See supra notes 239–244 and accompanying text.
254 See Gates, 462 U.S. at 238.
of the investigation is intelligence-gathering rather than law enforce-
ment, the Attorney General may authorize electronic surveillance or
physical searches without a warrant. The national security exception to
the Fourth Amendment allows for warrantless searches or surveillance
on the basis of uncorroborated tips from informants, without any show-
ing to a judge that the information is reliable or that the informant has
not provided such information to serve ulterior motives. Furthermore,
the President has authorized a program under which the National Se-
curity Agency has conducted warrantless electronic surveillance on
hundreds of occasions, without following even the minimal require-
ments of FISA. Such conduct poses a threat to individual privacy of
Americans whose communications may be intercepted in the course of
such surveillance.

In addition, successive Attorneys General have seen fit to issue
guidelines specifically establishing the manner in which federal agents
may engage high-level informants. But new guidelines evince a policy
decision that federal agents should not be bothered with practical rules
for handling confidential informants in national security investigations.
The rules established by the Informant Guidelines regarding immunity,
payments, bribes, and the nature of relationships between federal
agents and their informants do not apply where the target is an inter-
national terrorist. For now, this may be a tolerable situation, due to the
urgency and difficulty of recruiting informants for counterterrorism
investigations. It may well be that the threat posed by foreign terrorists
is greater than any threat from homegrown criminals in the past. Yet
even if this is true, vigilance is required to ensure that law enforcement
agents do not use informants in a way that violates individual privacy or
oversteps proper investigative boundaries.

Daniel V. Ward