January 2006

The psychology of leaking national security secrets: Implications for homeland security

The Psychology of "Leaking" Sensitive Information

Implications for Homeland Security

NOT SECRET

Need to know Only!

Randy Borum
University of South Florida

R. Scott Shumate
U.S. Department of Defense

Mario Scalora
University of Nebraska

The Homeland Security
Review
A Journal of the Institute for Law & Public Policy
CALIFORNIA UNIVERSITY OF PENNSYLVANIA VOL. 1, NO. 2, FALL 2006

Contents

The Homeland Security Review, Vol. 1, No. 2 (Fall 2006).

Psychology of "Leaking" Sensitive Information: Implications for Homeland Security

RANDY BORUM, University of South Florida

R. SCOTT SHUMATE, Directorate of Behavioral Sciences, Counterintelligence Field Activity (CIFA)

MARIO SCALORA, University of Nebraska

Introduction

Leaks of sensitive information, whether intentional or unintentional, can threaten US national security (Bruce, 2003; Hurt, 2001). A recent classified study of the impact of media leaks on homeland and national security documented numerous instances in which actual — and sometimes substantial — harm has occurred (Bruce, 2003; Hoekstra, 2005). (Portions of this study were published in a classified appendix to the Silberman-Robb Commission's Report on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction.) "The fact of the matter is, some of the worst damage done to our intelligence community has come not from penetration by spies, but from unauthorized leaks by those with access to classified information." (Hoekstra, 2005). Bruce (2003) similarly concludes "unauthorized disclosures of classified intelligence pose a serious, seemingly intractable, problem for US national security" (p. 39).

There is no official definition of "leaking" in US statutes or policy, but in security and intelligence contexts, the term generally refers to unofficial and/or improper public disclosure of otherwise sensitive, confidential or officially classified information, by someone with legitimate access, typically to, or through, journalistic or media interlocutors. Sometimes individuals with legitimate access to sensitive security information (insiders) disclose it to the media, notwithstand-

The views and opinions expressed in this article are those of the authors and do not represent the official policy or position of the Department of Defense, or the U.S. Government.

ing the existence of rules, policies, laws, and ethical principles that proscribe such behavior (Son, 2002). The compromised information and the people who disclose it are commonly referred to as "leaks."

Although espionage is the most robust threat to the security of national defense secrets, leaks can also pose a substantial risk (Gannon, 2001; Hitz, 2005; Owen, 2002). Espionage is "the act of obtaining, delivering, transmitting, communicating, or receiving information about the national defense with an intent, or reason to believe, that the information may be used to the injury of the United States or to the advantage of any foreign nation" (see Chapter 37 of Title 18, sections 792-798 and Article 106, Uniform Code of Military Justice). There is some precedent set by the US Department of Justice for applying espionage laws to leakers, but this practice is neither common nor well-established in law.

Depending on definitions, the distinction between leaking and espionage can be ambiguous. Some would argue that espionage is an extreme form of leaking. Others, using a more focused definition, view espionage as a different form of behavior. The distinction in those cases is a matter of intent. An individual committing espionage does so with "intent, or reason to believe, that the information may be used to the injury of the United States or to the advantage of any foreign nation." Leaks, in contrast, may not be divulged with that type of intent or foreknowledge, especially leaks made to media or public outlets. Indeed, a leaker's motives for public disclosure are likely to differ from those for clandestine, strategic disclosure to an adversary or foreign power. Regardless of intent, however, improper disclosure can result in harm to homeland defense or our nation's assets.

The systemic context in which security leaks occur is primed by inherent tensions that exist between institutions of national security and the media regarding the nature and degree of government and defense-related information that should be available to the public (Aftergood, 2002; Theoharis, 1998). Homeland security agencies and the counterintelligence community are committed to protecting information that could disadvantage U.S. interests or compromise defense or intelligence operations and assets (Owen, 2002; Relyea, 2006; Wettering, 2000). The protection of critical infrastructure and key assets (including human assets) has been explicitly designated as a critical mission area in the U.S. National Strategy for Homeland Security (Office of Homeland Security, 2002). Journalists and media — though typically not with reckless disregard for national security interests — are equally committed to acquiring and disseminating to the public as much information as possible regarding the operation and activity of its government.

There is little disagreement about the fact that government-related information is regularly exchanged between officials and reporters, but there is disagreement regarding its propriety. In arguing that information leaks to the press are a "form of communication," Richard Kielbowicz (1979/1980) provides some historical context for understanding the scope and connotations of the term as it is used today:

> The term "leak," coined in the early twentieth century, was originally applied to inadvertent slips in which information was picked up by reporters. The word quickly acquired a broader, more active meaning: any calculated release of information to reporters with the stipulation that the source remains unidentified. (p. 53)

The idea that leaks are a commonly accepted, if not legitimate, form of communication between the government and the press was reasserted in 2000 in a letter to then-President Clinton that was jointly signed by the chief editors at *The New York Times*, the *Washington Post*, the Newspaper Association of America, and *CNN*. They were urging him to veto a provision that would impose criminal penalties for unauthorized disclosures of classified information. They proposed that "the 'leak' is an important instrument of communication that is employed on a routine basis by officials at every level of government."

While media leaders may view them as "important instruments for communication," Tant (1995) has characterized unauthorized disclosures of secret government information as "acts of irresponsibility or betrayal" (p. 197). Still others regard leaking as an act of treason. Appraising the ethics and pragmatics of leaking may depend upon a variety of factors such as: who is doing the leaking (e.g., status or role); the leaker's motive (e.g., to disclose official wrongdoing or to embarrass an opponent); the nature of the leak (e.g., officially classified or just politically loaded); and the recipient of the leaked information (e.g., reporter or representative of a foreign intelligence service).

We know from psychological research that secrecy is a normal part of everyday life, but that keeping secrets and concealing information can be cognitively and emotionally burdensome (Kelly, 1998; Lane & Wegner, 1995; Peskin, 1992). Do we routinely inoculate or adequately equip our secret keepers to defend against these burdens or do we simply tell them that they should? Isn't it reasonable to assume that the way we indoctrinate and oversee our secret keepers could affect their secret keeping behavior?

Researchers in the business field have studied employees' attitudes and behaviors regarding "trade secrets." Like the government, businesses have an array of procedures for protecting their trade secrets from public or competitive disclosure, most of which could be categorized as either "access restriction" (AR) or "handling procedures" (HP).

According to Hannah (2005) "ARs restrict employees' right of entry to certain areas of an organization's physical facilities, their rights to use sensitive documents and their means of copying them, and their rights to use computers and means of communication, . . . (whereas) HPs establish rules for what employees can and cannot do with trade secrets once they gain access to them" (p. 73). Interestingly, both types of protections don't affect employee behavior in the same way.

The more familiar employees are with ARs, the *weaker* are their felt obligations to maintain trade secrets. Conversely, the more familiar they are with HPs, the *more* they feel obliged to keep the company secrets (Hannah, 2005). Why this difference? Research evidence suggests that the nature and degree of trust an employee perceives from her or his employer is a key mediating factor in secret keeping (Fox, 1974; Malhotra & Murnighan, 2002; Robinson, 1996; Rousseau, Sitkin, Burt, & Camerer, 1998). The findings are based in the theory that employees develop often tacit "psychological contracts" with their employers based on their expected reciprocal obligations.

> When employees see themselves as being in high-trust relationships with their employers, they are more likely to have psychological contracts that include high levels of personal obligations; but when employees perceive they are in low-trust relationships, they are more likely to have minimal definitions of their own obligations. . . . ARs in effect signal to employees that the company does not believe they have the discretion or commitment needed to follow the necessary procedures if entrusted with their firm's secrets. . . . HPs signals(s) to employees that their employers trust them sufficiently to provide them with access to trade secrets (Hannah, 2005, p. 74).

This fascinating line of research raises a host of intriguing questions for governmental secret-keeping policies. The transactive effects of trust dynamics can be influenced by a variety of security policies and procedures. An early analog business study divided subjects, randomly designating them as either supervisors or subordinates. The supervisors were tasked with "monitoring" certain subordinates. Not unexpectedly, the supervisors came to trust the "monitored" workers less (Strickland, 1958). Other research has adapted the psychological contract findings and attempted to make those contracts explicit. The effects were the reverse of what was intended. The explicit behavioral contracts appeared to *reduce* trust between the parties, thereby reducing the employee's feeling of obligation to the company (Malhotra & Murnighan, 2002).

The lesson is that the way employees perceive the meaning of secret protection policies is as important or more important than the policymaker's intent — at least as it relates to perceptions of trust. For example, research on employee monitoring has shown that employees feel and react differently to monitoring when they believe it is being used to help them or improve performance than when it being used punitively (Holman, Chissick & Totterdell, 2002). Indeed, when employees believe that secret protection policies — both ARs and HPs — are strongly enforced this also increases their felt obligation to maintain company trade secrets.

In summary, the psychological research on secret keeping suggests that leaking behavior may be best understood, by focusing not only on the leaker, but also on the situation, intended recipient, target, and the setting in which the behavior occurs. The setting, in this context, is determined by two conditions; (a) the threat environment, and (b) the OPSEC or Operational Security environment. Regarding the threat environment, consideration must be given to the fact that people and agencies exist with a range of motives that recruit, encourage, and elicit leaks. Media, in particular, will protect the identity of their sources (Melanson, 2001; Sigal, 1973). The OPSEC environment is a significant factor for both intentional and unintentional leaks. It is the first line of prevention. To use leaking as a tactic requires very little skill or sophistication, so screening and co-worker awareness become important components of an effective defense (Bruce, 2003).

Moreover, a substantial body of psychological research more broadly indicates clearly and consistently that personality factors will only explain or predict a limited amount of any behavior, and that situational (and often contextual) factors typically exert much more influence (Kurtines, 1986). Jointly examining factors influencing the leaker, situation, and setting will better illuminate the leaking process and its underlying motivational considerations. This should lead to a more nuanced and complex understanding of the phenomenon across the spectrum of its diverse manifestations, which may also form better policies and interventions designed to protect our nation's sensitive secrets.

Toward a Motivational Typology of Leaking

In the following section, we offer some very preliminary observations and analysis of "leaking" from a behavioral perspective — focusing on "motivation" as a critical variable — within a framework of counterintelligence objectives and principles. "Counterintelligence means information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations or persons, or international terrorist activities, but not including personnel, physical, document or communications security programs" (Executive Order 1233 — United States Intelligence Activities, 3.4(a), 1989).

The following assumptions guide our behavior-based CI framework for understanding leaking:

- Sensitive information pertaining to US national security and critical US assets can be improperly used as a commodity and must be protected;
- Leaked information does not have to be formally classified to be improper or harmful; and
- Degree of harm is a consequence, not a characteristic of a leak.

With an understanding of the framework, what follows is a behavioral perspective on, and analysis of, leaking behavior, focusing on the key dimensions of intent and motivation. While there are no known empirical, scientific studies of leaking in the counter-intelligence field, anecdotal accounts suggest its manifestations are fairly diverse. Leakers' motives may range from the altruistic to the malevolent. The behavior may be impulsive or carefully planned. Leakers may act on their own initiative, or under orders from others.

At the most fundamental behavioral level, leaking can be classified and understood along a continuum of intent. At one end of the continuum, would be leaks that are purely inadvertent. At the other end, would be cases where the disclosure was planned, knowing, willful, and malevolent (perhaps including espionage). The Honorable Pete Hoekstra (2005), Congressman from Michigan and Chairman of the House Permanent Select Committee on Intelligence has used the descriptive axis of intent, broadly classifying leaks into three categories: accidental, deliberate and espionage-related.

Following this line of reasoning, the first order distinction in our proposed behavioral typology is based on *level of intentionality* — that is, whether the leak was intentional or unintentional. Either type can cause harm, of course, but the behavioral principles for understanding, identifying, and preventing each are likely to differ. Within the unintentional category, leaks may be made unknowingly, negligently, or as a result of impairment.

The second order distinction is based on causality or *motivation*. In the intentional category, leaking may be viewed most effectively as a tactic for accomplishing an objective. Observations from Washington "insiders" suggest that the most common motivation for leaking may be political — using that term in the broadest sense. In the 1980s, a former *New York Times* Pentagon reporter asserted that leaking is "a political instrument wielded almost daily by senior officials within the Administration to influence a decision, to promote policy, to persuade

Congress and to signal foreign governments." (Halloran, 1983, p. A16). More than 20 years later, Representative Hoekstra (2005) shares a similar observation that politicians and officials regularly use leaks in a variety of ways as a tactic to accomplish political objectives:

> It has become all too common—almost second nature—for people in Washington to leak information. Policymakers may leak for any number of reasons, such as to bring attention to a good news story or discredit a bad story. They may also leak information to gauge public interest on a new policy or issue. But some seemingly leak just because they can. These are the people, and especially those that have access to classified information, that we need to worry about.

To offer "political" motivation as an explanation for people's behavior in Washington, DC is almost tautological. Understanding how and why leaks occur and are used by officials requires an additional layer of motivational analysis. Stephen Hess (1984) proposed one of the first motivation-based typologies for politically-leaked secrets, with the following six categories — the ego leak, the goodwill leak, the policy leak, the animus leak, the trial-balloon leak, and the whistle-blower leak.

Understanding that political motivation may be a meta-explanation, our proposed typology focuses on common motivations for leaking national security information. Accordingly, we offer the following motivational explanations for leaking — Financial, Ego Driven, Altruistic, Vengeful, or Ideological.

Unintentional Leaks

Unintentional leaks are not willful violations of security rules and measures. They are not planned, directed or malevolent, although they certainly can cause harm. Three main types of unintentional leaks are as follows:

- *Unknowing*: The leak occurs without the leaker knowing that: (a) the information was sensitive or protected; or (b) the sensitive or protected information was disclosed.
- *Negligent*: The leaker is aware that the information is sensitive and that disclosure would be improper, but divulges as a result of carelessness, artifice, or failure to follow proper security procedures.
- *Impaired*: The leaker knows the information is sensitive and that disclosure would be improper, but divulges due to impairment in his or her mental or volitional capacities, usually as a result of intoxication or mental disorder.

Intentional Leaks

Intentional leaks involve willful violations of security rules and measures, though the motives for them vary. They may be carefully planned and concealed or impulsive. They may be self-initiated or directed by others. Although all malevolent leaks are intentional, the *motivation* for all intentional leaks is not necessarily malevolent. The degree of intended malevolence, however, does not necessarily correspond to the degree of harm that the leak may cause.

Intentional leaking, as we noted, is a tactic. It is instrumental behavior, meaning that it is a means to an end. The leak itself is simply the instrument, apparatus or weapon of the chosen means.

Because intentional leaking is instrumental, the key distinguishing characteristic between the various types is motivation behind the action, including the type of goal it is intended to accomplish. Understanding the role of motive in leaking behavior is critical. The motive often determines what sensitive information will be disclosed and to whom. In most cases, however, motives for leaking are complex and overlapping (Gelles, 2005; Hess, 1986). Leaking, when there is foreseeable harm, requires most people to rationalize or justify their behavior (Bandura, 1999), potentially providing additional insights for prevention and investigation.

With the caveat that motivations are rarely simple and singular, we propose the following five types of intentional leaks — financially motivated, ego driven, altruistic, vengeful and ideological.

Financially motivated leaks occur when the leaker discloses sensitive information for financial gain. This is often a presumed and actual motive for espionage, but it offers an incomplete explanation. Gelles (2005) suggests that "people commit espionage not just for money, but in a desperate attempt to fulfill complex emotional needs."

When an Ego Driven leak is the motive, the leaker is motivated by incentives for personal gain in perceived status or power. In some cases, the leaker provides classified information simply to prove to others that he or she possesses sufficient importance to have access to such information. Some leakers in this category may have narcissistic (i.e., overvaluing one's self, value, and abilities) personality features.

When the leaker believes that, by disclosing the sensitive information, he or she is serving some "greater good" and *Altruistic* theory is behind the leak. Leakers in this category may believe, for example, that nondisclosure of certain information is causing harm to others, causing an injustice (e.g., that someone is "getting away" with improper behavior), or even compromising national security. This type might include those leaks that some may characterize as "whistleblowers". The concept of whistle blowing is more ethically complex than it may appear on the surface (Near & Miceli, 1996). Near and Miceli (1985) who have studied the phenomenon extensively, but primarily in the corporate content, have defined whistle blowing as "the disclosure by organization members (former or current) of illegal, immoral or illegitimate practices under the control of their employers, to persons or organizations that may be able to effect action." (p. 4). Generally, the tradeoffs involved in leaking national security information for purposes of whistle blowing may be more vexing than in the business world. It is not necessarily true that leakers of this type are less morally culpable or purer in heart than other types. Concurrent elements of ego-driven and vengeful motives could potentially color an "Altruistic" leaker's appraisal of her or his situation.

Vengeful leaks occur when the leaker is motivated by revenge or anger toward a particular target. The primary goal of the leak is to harm or embarrass an individual, group, agency or nation. Vengeful leaking may be done competitively — to advance one's own relative status or position relative to that of the leak targets — or with pure malevolence intended to harm the leak target as punishment or retaliation, and perhaps to deter others, collaterally, from transgressing against the leaker in the future.

The Ideological leaker is motivated by an ideological or political objective. The primary goal of the leak is to advance a cause or to injure opponents of the cause. Arguably, leakers in this category are similar to those who commit espionage; however, espionage, unlike leaking, less commonly involves disclosure to public or media information sources. The motivational profile of the ideological leak may, therefore, overlap with the Vengeful or Altruistic.

Case Example:

To illustrate the motivational complexity of leaking behavior, and the proposition that the motive in these cases is rarely "pure" (referring to the mixture, not the morality) consider the facts of a hypothetical, but not uncommon case. A longstanding government employee and faithful public servant disagrees with her organization's shift in policy and activity following a post-election change in administration. She believes that public reports from her agency are being distorted or misrepresented to disguise inefficiency or actual harm. In her "heart of hearts" she believes that these new policies and activities are harming Americans, generally, or some specific target group (e.g., senior adults, elementary school children, etc). She has raised her concerns in agency leadership meetings and in one-to-one conversations with a couple of the agency's leaders, but is characteristically placated or "shut down." She concludes her internal options for redress have been exhausted. She decides, to "anonymously float" some of her concerns by a newspaper reporter who has covered her agency's beat for more than a decade.

Assuming that our public servant was not seeking or accepting money in exchange for the information she offers to the reporter, we could parse out the financial element of her motivational profile. While financial considerations are common in espionage, they are relatively uncommon in more routine government leaks. But what of the other motivational elements? Is there "political" motivation? It certainly appears so, in that she is attempting to affect changes in governmental policy either directly or indirectly by manipulating conditions that might cause those policies or policy-makers to change. Is it ego-driven? It certainly would not be surprising to find that a career public servant who has been repeatedly dismissed and "shut down" within her agency felt disrespected and suffered what some psychologists might call a "narcissistic injury" (i.e. feelings of humiliation or degradation that come from "losing" or being criticized). Affirmations from the knowledgeable, veteran reporter may help to allay some of the damage inflicted on her self-esteem. Is she thinking to herself: "I feel devalued by my agency. I know the reporter will be sympathetic to my position. Maybe talking to him will make me feel better about myself." Probably not. Might those dynamics influence the employee's behavior, however? It's difficult to see how they could not.

If she felt dismissed and devalued — perhaps even betrayed — by her agency's reactions to her concerns and dismayed by their disregard for the harm they had caused (in her view), it does not seem unlikely that she might feel angry toward the agency — or at least certain senior leaders. Even as a loyal employee, the opportunity to expose the incompetence or impropriety of those who aggrieved her — perhaps even embarrass them — may understandably hold some appeal. It is unlikely she would put forward a vengeful motive as "the real reason" for the leak. Indeed, it may not be. Viewing the situation through the lens of motivational theory, however, it would seem to have more "approach" than "avoidance" qualities. If the facts were conversely applied — that is, if public disclosure would cause embarrassment or harm to her closest friends and colleagues — it would be easy to see the conflict (approach-avoidance) that could produce for her. That it might embarrass her detractors may be "icing on the cake", but it is nonetheless a real part of the motivational calculus.

The employee probably views her own motivations principally as "altruistic" and perhaps secondarily as ideologically driven. She may very well regard herself as a whistle-blower, maybe even a crusader. She believes the agency's actions are causing harm that they refuse to redress. She may feel compelled by a sense of moral or social obligation to act in order to prevent further harm from occurring or to protect those who she believes are being adversely affected. Her appraisal of "harm" or the cost-benefit analysis of the policies may be influenced by her ideological views and assumptions. Maybe she entered government service with the ideal of serving a "cause" that she feels is now being violated by those in power. Even if one were to classify this case as Altruistic within the motivational typology, it is clear that the employee's behavior actually reflects constellation of motives. Understanding this complexity and the ways in which motivational factors affect each other can help to advance efforts to prevent leaks that may threaten homeland security.

Preventing Risky Leaks

Many positions and proposals are currently "on the table" to address this critical security issue. Leaking behavior, in its various forms, however, must be adequately understood, before it can be effectively blocked or managed. Leaks occur for many reasons, and intentional leakers have a range of motivations. Different kinds of leaks require different kinds of prevention strategies.

Prevention and risk assessment for leaks should examine inhibiting as well as motivating factors. It is possible to intervene in this problem at a variety of levels, but it is first necessary to understand which kinds of leaks are most common and most hazardous, how and to whom they occur, and how intentional leakers navigated around the barriers (e.g., rules and sanctions) both logistically and psychologically.

Some enormous overarching policy questions and issues lie embedded in the task of preventing national security leaks: How do (and should) we designate information that should be considered a national security secret? How do we decide to whom we should entrust that information? How do we monitor whether they are responsible stewards of that trust? How do we educate and prepare them for the task of keeping national security secrets? How do those so entrusted understand the procedures and rationale for keeping the secrets and likely consequences for revealing them?

One prominent school of thought is that new laws imposing serious criminal penalties for leakers are needed to protect our nation's secrets (Bruce, 2003; Hurt, 2002). Bruce's (2003) observation of "permissive neglect" suggests that our history of under-enforcement of secrecy violations may decrease the obligation that other government employees feel to closely guard confidential information. He argues "unless comprehensive measures *with teeth* are taken to identify and hold leakers and their publishing collaborators accountable for the significant, often irreversible, damage that they inflict on vital US intelligence capabilities, the damage will continue unabated" (Bruce, 2003, p. 49). Newly crafted legislation might reasonably be part of a comprehensive program to prevent leaks of sensitive or classified information that could threaten national security. Tougher laws, however, should be seen as a tool, not as a total solution. A host of criminological research has already demonstrated that increasing legal penalties alone has, at best, a modest effect on law breaking behavior. The certainty of sanctions is typically a greater deterrent than the severity of the sanctions. Changing perceptions of the likelihood of sanction, however, requires more than a change in the law.

Perhaps a "public health" model provides a better guide to success. Following such an approach, we might: (1) define and understand leaking by investigating the nature, magnitude, scope, characteristics and consequences of past leaks; (2) seek, through systematic inquiry to learn the causes and correlates of leaking, including what factors might increase or decrease the likelihood that it will occur; (3) use that knowledge to design, implement and evaluate interventions to prevent and deter leaking; and (4) implement the "effective" interventions as widely as possible across the government. This approach does not imply that new laws or tougher sanctions necessarily should or should not be used. It does imply, though, that such changes should be informed by a clearer understanding of leaking behavior and — like all interventions — should be evaluated to determine how well they work. Of course, there may be other reasons to change laws and penalties, but our focus here is on prevention.

A program of CI-based behavioral research aimed at understanding and helping to prevent leaks is possible with adequate access and support. An effective research program might systematically examine a sample of past leaking incidents with careful attention and consideration given to analyzing the leaker, the intended target, the work and or personal situation surrounding the incident, how leaking was chosen as a strategy, how the information recipient was selected, the setting in which the leak occurred. Psychological frameworks such as the "Theory of Planned Behavior" (Ajzen, 1998) could provide overarching conceptual guidance for understanding personal and contextual pathways to intentional leaking.

Conclusion

Leaking sensitive and classified information is a pernicious, but perennial problem. Without some type of action, the governmental and public ethos is unlikely to change and behavior is unlikely to diminish or go away. A broad range of interests and perspectives are represented in the national conversation about governmental "leaks." Our suggestions don't resolve many of the murky questions in this critical debate. We believe, however, that diverse interests can best be served by elucidating an informed understanding of this national security problem before reflexively implementing a host of measures that may be costly, misguided, or ineffective. In *Haig vs Agee (*453 U.S. 280, 1981) Justice Burger noted "It is 'obvious and unarguable' that no governmental interest is more compelling than the security of the Nation." Protecting that interest deserves nothing short of our best efforts.

References

Aftergood, S. (2002). On leaks of national security secrets. *National Security Studies Quarterly, 8,* 97-102.

Ajzen, I. (1998). *Attitudes, Personality and Behavior.* Chicago, Illinois: The Dorsey Press.

Bruce, J. (2003). Laws and leaks of classified intelligence: The consequences of permissive neglect. *Studies in Intelligence, 47,* 39-49.

Fox, A. (1974). *Beyond Contract: Work, Power, and Trust Relations.* London: Faber and Faber Limited.

Gannon, J. (2001). *Stealing secrets, Telling Lies: How Spies & Codebreakers Helped Shape the Twentieth Century.* Potomac Books.

Gelles, M. (2005). Exploring the mind of the spy. *Employees' guide to security responsibilities: Treason 101.* Washington, DC: Defense Security Service. Available online at: http://www.dss.mil/training/csg/security/Treason/Mind.htm

Halloran, R. (1983, January 14). A primer on the fine art of leaking information. *New York Times,* p. A16.

Hannah, D. (2005). Should I keep a secret? The effects of trade secret protection procedures on employees' obligations to protect trade secrets. *Organization Science, 16,* 71-84.

Hess, S. (1984). *The government/press connection: Press officers and their offices.* Washington, DC: Brookings.

Hitz, F. (2005). The myths and current reality of espionage. *International Journal of Intelligence and CounterIntelligence, 18,* 730-733.

Hoekstra, P. (September 6, 2005). *Secrets and Leaks: The Costs and Consequences for National Security.* Heritage Lecture #897. Washington, DC: The Heritage Foundation.

Holman, D., Chissick, C., &. Totterdell, P. (2002). The effects of performance monitoring on emotional labor and well-being in call centers. *Motivation and Emotion, 26,* 57–81.

Hurt, M. (2001). Leaking national security secrets: Effects on security and measures to mitigate. *National Security Studies Quarterly, 7,* 1-38.

Jost, K. (December 2, 2005). Government secrecy: Is too much information being kept from the public? *The CQ Researcher, 15*, 1005-1028.

Kelly, A., Klusas, J., von Weiss, R., & Kenny, C. (2001). What is it about revealing secrets that is beneficial? *Personality and Social Psychology Bulletin, 27*, 651-665.

Kielbowicz, R. B. (1979/1980). Leaks to the press as communication within and between organizations. *Newspaper Research Journal, 1*(2), 53–58.

Kurtines, W. (1986). Moral behavior as rule governed behavior: Person and situation effects on moral decision making. *Journal of Personality and Social Psychology, 50*, 784-791.

Lane, J. D., & Wegner, D. M. (1995). The cognitive consequences of secrecy. *Journal of Personality and Social Psychology, 69*, 237-253.

Linsky, M. (1991). *How the press affects federal policymaking*. New York: Norton.

Malhotra, D. & Murnighan J. K(2002). The effects of contracts on interpersonal trust. *Administrative Science Quarterly, 47*, 534–559.

Melanson, P. (2001*). Secrecy wars: National security, privacy, and the people's right to know*. Brassey's.

Mencher, M. (1997). *News reporting and writing* (7th ed.) Madison, WI: Brown & Benchmark.

Near, J. & Miceli, M. (1985). Organizational dissidence: The case of whistle-blowing. *Journal of Business Ethics, 4: 4*.

Near, J & Miceli, M. (1996). Whistle-blowing: Myth and reality. *Journal of Management, 22*, 507-526.

Office of Homeland Security (July, 2002). *National strategy for homeland security*. Washington, DC: The White House Office of Homeland Security.

Owen, D. (2002). *Hidden Secrets: A Complete History of Espionage and the Technology Used to Support It*. Firefly Books Ltd.

Peskin, J. (1992). Ruse and representations: On children's ability to conceal information. *Developmental Psychology, 28*, 84-89.

Relyea, H. (June 26, 2006). Security classified and controlled information: History, status, and emerging management issues. *CRS Report for Congress* # RL33494. Washington, DC: Congressional Research Service.

Robinson, S. (1996). Trust and breach of the psychological contract. *Administrative Science Quarterly, 41*, 574-599.

Rousseau, D., Sitkin, S., Burt, R. & Camerer, C. (1998). Not so different after all: A cross-discipline view of trust. *Academy of Management Review, 23*, 393-404.

Sigal, L. V. (1973). *Reporters and officials: The organization and politics of newsmaking*. Lexington, MA: Heath.

Son, T. (2002). Leaks: How do codes of ethics address them?. *Journal of Mass Media Ethics, 17*(2), 155-173.

Tant, A. P. (1995). Leaks and the nature of British government. *The Political Quarterly, 66,* 197-209.

Theoharis, A. (Ed.) (1998). *A culture of secrecy: The government versus the people's right to know*. University Press of Kansas.

Vrij, A., Paterson, B., Nunkoosing, K., Soukara, S., & Oosterwegel, A. (2003). Perceived advantages and disadvantages of secrets disclosure. *Personality and Individual Differences, 35*, 593-602.

Wettering, F. (2000). Counterintelligence: The broken triad. *International Journal of Intelligence and CounterIntelligence, 13*, 265-300.