
Kenneth J. Ryan

Follow this and additional works at: https://repository.law.uic.edu/jitpl

Part of the Computer Law Commons, Internet Law Commons, and the Science and Technology Law Commons

Recommended Citation


https://repository.law.uic.edu/jitpl/vol25/iss4/10

This Symposium is brought to you for free and open access by UIC Law Open Access Repository. It has been accepted for inclusion in UIC John Marshall Journal of Information Technology & Privacy Law by an authorized administrator of UIC Law Open Access Repository. For more information, please contact repository@jmls.edu.
INFORMING THE ENEMY: FEEDING THE COUNTER-INTELLIGENCE NEEDS OF OUR ADVERSARIES

KENNETH JAMES RYAN, Ph.D.*

I. BALANCING SECRECY AND OPENNESS

A significant challenge to the intelligence executive is defining his or her professional role as chief of an organization with diverse purposes, goals and objectives. This is particularly true for those executives who serve at the pleasure of a political figure, or for a succession of political figures with varied priorities. Criminal intelligence has largely been spared from political interference in the West, at least in comparison with foreign and defense intelligence; however, since the terrorist attack at the 1972 Munich Olympics, the efficacy of counter-terror efforts by European law enforcement has become a political issue. With increasing frequency, the products of criminal intelligence operations become front-page news, especially in regard to thwarted terror plots. When terror plots are not thwarted and violence erupts, it has become commonplace among media, politicians, and the public to place first blame at the door of intelligence agencies, if not the agency executives themselves, for failing to detect and stop the terrorist act before it occurred.1 Therefore, over the past quarter-century the formerly (and comparatively) insulated position of the criminal intelligence executive has crept into an uncomfortable spotlight of scrutiny.

Whether this is fair practice or not is difficult to say; however, in an environment where secrecy serves the daily task of generating intelli-

---

* Dr. Kenneth James Ryan is the director of the joint doctorate with the University of California-Davis in Forensic and Behavioral Sciences at California State University-Fresno. He is a specialist in international criminal intelligence and comparative justice. Prior to joining CSUF, he instructed counter-terror, intelligence and global organized crime studies in St. Louis at Washington University and the University of Missouri. He has lectured at other colleges and universities on political science. He currently serves as a private consultant in fiscal management of government intelligence operations. He received his Ph.D. in Interdisciplinary Studies in Political Science from Washington University in St. Louis.

gence, particularly in information collection processes, exposing operational detail is rarely viewed as a positive venture. Thus, the intelligence executive must strike a careful balance between transparency and secrecy.2

II. PROVIDING USEFUL COUNTER-INTELLIGENCE TO THE ADVERSARY

Countering harmful disclosures by media and ill-advised politicians, while remaining transparent in a liberal democracy proves to be a delicate balancing act for the intelligence executive. The executive's ability to find and maintain this equilibrium may determine an agency's success or failure, particularly in regard to broad political conciliation and public perception. For example, a US Congressman interviewed by newspaper reporters after a Pacific Theater tour offered one of the more visible intelligence gaffs of World War II. When reporters asked about the naval war in the Pacific, the Congressman related that there was little to worry about, since the Japanese had been dropping depth charges too shallow to do significant damage to the American submarine fleet. In turn, and predictably one might argue, the press printed the story and ultimately the information made its way back to Japan as open source intelligence. The Japanese Navy corrected their anti-submarine tactics, and as a direct result approximately 800 US submariners lost their lives.3

Although this lesson is more than six decades old, its mistakes are often repeated. Another such gaff occurred on a cable television news network not long after the 2000 bombing of the USS Cole in Yemen. With a silhouette of the Cole on an easel, a retired US Navy Command Officer pointed to indicate where the Cole had been bombed, an attack resulting in the deaths of seventeen sailors. The Officer said, pointing to a different part of the ship, "If the terrorists had placed the bomb here instead, the entire ship would have blown up."4 As of this writing, there have been no similar attacks on US warships in that region; however, the retired naval officer armed the terrorists with a better strategy for next time by providing critical open source intelligence.

Law enforcement is not immune from such gaffs where secrecy and openness collide. In the late 1970s, the St. Louis County, Missouri Superintendent of Police ordered a photograph of the entire department en

2. ABRAM N. SHULSKY & GARY J. SCHMITT, SILENT WARFARE: UNDERSTANDING THE WORLD OF INTELLIGENCE 144-46 (Brassey's, 3d ed. 2002); DANIEL P. MOYNIHAN, SECRECY: THE AMERICAN EXPERIENCE ch. 6 (Yale University Press, 1998).


4. Paraphrasing; so as not to compound the gaff, this cite is deliberately omitted.
masse. The “family photograph” would be made available to the public at no charge. Stacks of photographs were placed in the Old Court House building (the same building that housed the County Jail) for public acquisition. Subsequently, organized crime, drug dealers, illicit fences, gambling operators, among many other criminal entrepreneurs used the readily available photograph to identify undercover police attempting to infiltrate criminal organizations, crippling critical covert operations.5

The transparency versus secrecy dichotomy lingered over time (or over many lessons) with police executives, investigators and agents vying for cable and local television face time whilst proudly divulging sensitive operational details without regard for future operations. One such incident centered on the 2007 kidnapping and murder of a woman whose body was located via the GPS system in her cell phone. A police officer that helped crack the case provided infinite detail to international cable television reporters regarding how a cell phone company is able to trace the whereabouts of the cellular instrument with a technique called pinging.6 For kidnappers (of all varieties and for all time to come), this information was priceless. Once kidnappers understand the pinging method, countermeasures are easily discernable. The investigative and intelligence damage done, not to mention the potential loss of human life in kidnappings not yet occurred, is incalculable.

Now, the question is whether the damage was caused with deliberation, by accident, or merely through poor planning. To suspect that the release of critical information is always deliberate and done with the intent to inflict harm, one might suppose there are malignant motives behind any disclosure. Therefore, one would assume the Ohio congressman was a Japanese spy; one must suppose the Superintendent of Police is in league with organized crime; and that the same officer who divulged cell phone tracking information is himself a kidnapper. Logically speaking, this is beyond doubtful as it presupposes that all who commit disclosures are deliberately in league with the adversaries.

However, in each of the above disclosure scenarios, the public release of agency operational detail yielded the damage. This key revelation is critical in understanding what can be done at the agency level to prevent vital counter-intelligence from falling into the hands of our adversaries through open sources. Whereas, there is very little done in law enforcement that rises to the level of requisite secrecy, particularly in the U.S. court system wherein justice relies on thorough discovery. Divulging operational detail in a court of law at the pointed end of a subpoena is far different than divulging operational detail on cable

5. From the author's own experience.
television broadcast to a worldwide audience: one is the result of legal process, the other the result of community relations in a transparent agency (optimistically) or of rank naivety. Thus, it becomes evident the intelligence executive must weigh the benefits of transparency versus an anticipated intelligence loss (i.e., the net loss of information value once it becomes public) to an adversary before such disclosures are made.

According to William Hucklesby, retired Commander of the Scotland Yard Anti-Terrorist Squad, “Disclosures . . . are often deliberately made by those who are politically motivated with the intention to compromise [operations]. There are numerous examples of such practices, which could lead to not only character assassination but also actual assassination.”7 Facilitating an adverse intentional disclosure requires two elements: a legitimate intelligence consumer and a medium to serve as an open source for the opposition by publishing information or intelligence illicitly acquired. Without delving into the moral question regarding whether a medium should publish illicitly acquired intelligence, a consumer who wishes to release purloined intelligence likely would not have to go far to find a willing accomplice.8

It is essential that those in the business of intelligence anticipate that legitimate consumers may, at times, be at cross-purposes with the agency and could actively work against it. Furthermore, the release of information to any intelligence consumer bears a certain risk that disseminated intelligence may be used deliberately against the originating agency or against other sections of government. This issue illuminates yet another difference separating criminal intelligence from other varieties, particularly foreign and defense intelligence. The difference makes criminal intelligence far more vulnerable to open source intelligence gains by adversaries. Simply put, the difference is that upon the release of critical and guarded information into the open from a criminal intelligence source, most often there is nothing the intelligence executive can do about it in legal retribution.

In U.S. foreign and military intelligence services, there are nearly always codified prohibitions regarding unauthorized disclosure of protected or guarded information. Also, in European law enforcement, except for certain civil rights prohibitions, it is rare that an unauthorized and deliberate disclosure of sensitive intelligence (relating narrowly to a law enforcement operation) would have legal ramifications for the source. Therefore, a deliberate and unauthorized disclosure of operational detail, even detail that may have lethal consequences, most often

7. Letter from William Hucklesby, to author (June 27, 2007) (on file with author).

can be made with impunity by those who would seek to damage an agency, derail ongoing operations, or even deliberately endanger lives. That these potentially dangerous and damaging disclosures can be made public without legal consequence is not lost on the media or on politicians. For as long as there is no legal remedy by government for one who intentionally sabotages a criminal intelligence operation, the practice will doubtlessly continue to serve the motives of politics and benefit those who commit crimes.

Still, the generation of secret intelligence in a law enforcement agency must contend with issues of transparency that are at the heart of a liberal democracy. For example, one cannot dismiss the litany of human rights abuse by the East German Ministerium für Staatssicherheit (Ministry for State Security, a/k/a Stasi) of the last century. Neither can be dismissed the contemporary ethical issues of human rights violations in extraordinary rendition, in which political enemies of the West are kidnapped, taken to foreign locations and tortured for information or murdered under the premise that the practice does not violate domestic law.

The absence of institutional transparency veiled by a cloak of secrecy generates public suspicion and distrust in its institutions, particularly in question that its own law enforcement may be corrupt or abusive. Therefore, when deliberate and harmful disclosures are made without consequence, public opinion is the ultimate arbiter on the motives of the source, i.e., whether disclosure was intended to enrich the opposition or merely to enhance transparency.

III. DISCLOSURES VERSUS LEAKS

If one is to surmise intelligence disclosures are not intentional and instead mere accidents, a slip of the tongue in other words, then one must suppose that disclosing critical operational details takes but an unguarded moment. An accidental release presumes the speaker blurted

---


12. STEVEN J. CIMBALA, INTELLIGENCE AND INTELLIGENCE POLICY IN A DEMOCRATIC SOCIETY 56-57 (NY: Transnational, 187); Moynihan, supra note 2, at 22-29 (stating both in regard to conspiracy/corruption).
out something he or she otherwise would have known better than to divulge or perhaps was caught off-guard for a moment and made some harmful yet inadvertent revelation. An accidental release of information also may include passing on information that otherwise seemed harmless. Examining damaging disclosures, one must first note the difference between a disclosure and a leak. Indeed, one may consider the problem in much the same manner as one might view one's own plumbing.\textsuperscript{13} A disclosure is a deliberate turning of the information faucet with specific and known quantities of information or intelligence (i.e., analyzed information) released. In the context of a disclosure, there is no presumption of legality, illegality or propriety in the release, and the consequences can be either harmful or not. A disclosure is presumed to be a deliberate release of guarded information to the public by one who is authorized to possess it. A leak, on the other hand, is an unauthorized or unintended release of guarded information, much in the same way that one does not intend that a pipe might leak.

For example, and diverting from criminal intelligence to foreign intelligence for illustration, if a Foreign Service Officer discloses the nature, purpose, and schedule of an upcoming mission abroad, this may provide important information to whatever forces oppose such a visit. On the other hand, if a Foreign Service Officer discusses his mission abroad with a spouse, who subsequently discloses the nature, purpose, and schedule to a valet— who is a spy—the information was leaked to the opposition. Simply put, the disclosure was deliberate; however, the leak was not. In either case, the opposition receives a net gain of information with minimal cost, the first with deliberation on the part of the source and the second through art. Of the two options it is apparent that an inadvertent disclosure of guarded information is the most avoidable, if not the most common, as it should be controlled. Nevertheless, formal disclosures of guarded information that negatively impact law enforcement operations are a fairly common occurrence.

Hucklesby suggests that, although reasons may vary, inadvertent or damaging disclosures are most often "the product of naivety rather than the intent to deliberately compromise."\textsuperscript{14} When this is the case, a law enforcement agency becomes its own worst enemy. However, a law enforcement intelligence agency (or any intelligence agency) providing a naïve consumer with critical intelligence that, if disclosed, might cause irreparable harm neither reflects well on the consumer nor the intelligence apparatus itself. This is not to suggest that critical or sensitive

\begin{footnotes}

\end{footnotes}
intelligence should not be released to the appropriate consumer. Instead it is clear that release of intelligence to appropriate consumers or directly to the public must be carefully regulated, especially if the appropriate consumer is the public itself.

According to former South Yorkshire ("UK") Chief Constable Richard Wells, it is reasonable to place law enforcement, defense and military intelligence on the same footing in this regard. In any of these three, the opposition is viewed as the enemy and can benefit from collateral information, meaning information released for one purpose (e.g., to serve transparency), but instead enriches an enemy's intelligence about agency/department operations.\textsuperscript{15} Wells cautions that ethical issues are raised, particularly in regard to subterfuge in the public information role.

For example, Wells questions the efficacy of law enforcement subterfuge as a practice and cautions it is never proper; however, he adds that the public has no right to a blanket demand regarding operational detail. Subterfuge in this context is the offering of misinformation and is akin to lying to the public. As a public agency, law enforcement should never engage in this practice, as regaining the public trust is a long process once the falsehood has been exposed. Therefore, a law enforcement executive who deliberately engages in subterfuge has taken a step onto the slippery slope of community distrust. History is replete with anecdotes illustrating the fallacy of government subterfuge as a technique to cover (or attempt to cover) serious mistakes.\textsuperscript{16} In the wake of unethical behavior, the public likely shall view future subterfuge as a harbinger of misconduct, no matter the agency-perceived validity of the deception.

However, blocking information is a technique often used by military commands with considerable success in preventing collateral information from falling into the hands of adversaries. This technique is often accomplished by employing a Press Officer to conduct press meetings or, when conducted by military executives, more than one command rank or general officer is present. The phrase, "We cannot disclose operational detail," has become a lexicon in these military press conferences. However, this phrase is rarely heard from law enforcement- and to its own detriment.

One laudable exception to this unfortunate paradigm is the German Bundeskriminalamt (BKA), governed by a legal system in which nearly all operational detail is provided to the public through a prosecutor's office or a press office ("Pressestelle"). In the German criminal justice system there is no release of detail without considerable discussion among

\textsuperscript{15} Interview with Richard Wells (June 26, 2007) (on file with author).

\textsuperscript{16} CIMBALA, supra note 12, at 56. The reader doubtless can recall numerous examples such as the Tonkin Gulf in El Salvador and Vietnam era NIEs, to name a few.
vested parties participating in an inquiry. According to Erster Kriminalhauptkommissar Ranier Witt of the BKA, occasionally information is provided to the public in order to provoke a response from criminals or terrorists. This is not to say the BKA uses public subterfuge as a matter of course. However, it indicates that the BKA carefully uses operational information disclosure as a tactic.17

IV. REMEDIES

Three interconnecting remedies may be offered to prevent inadvertent disclosures. First of all, if disclosures are meant to be deliberate releases of information, perhaps deliberation should be returned to the formula. An executive team should be assembled any time a release of information to the public is proposed, and a Press Officer (or some incarnation thereof) should be appointed. The Press Officer should be a conduit of information and otherwise not inside the decision making loop, as is most often the case in government. With this practice, one person and one person alone answers media questions and is the representative of the agency or department. If the agency has an intelligence arm, it is vital this bureau participate as well. Finally, the prosecuting attorney/district attorney/U.S. Attorney should be involved as an equal stakeholder in any discussion at practical and policy levels regarding public disclosures.

Secondly, and above all other considerations, operational detail should never be released via media outlets without first vetting the information through appropriate intelligence, executive and prosecutorial players to ensure that counter-intelligence needs of our adversaries are not fed through open sources. Third, agency policies must be established and coordinated with others to ensure compliance with the above guidelines. This is crucial in protecting ongoing and future operations by guarding information from falling into the hands of our adversaries via open media sources.