THE USE OF CLASSIFIED INFORMATION IN TERRORISM TRIALS

Bruce M. MacKay*

"A strange game. The only winning move is not to play."[1]

I. INTRODUCTION

The most potent weapon America possesses in the battle against terrorism is information. Information provides the government the ability to determine terrorist intentions, identify terror actors, assess target vulnerabilities, and implement countermeasures. Information drives the government's decision cycle. The greater the depth and breadth of information at the government's disposal, the greater the range of options are available to the government.

Of all the information at America's disposal, arguably classified information represents the most precious information resource available. Classified information has the potential of disclosing details of terrorist intentions while identifying both terror actors and those who support them. Additionally, it has the potential to pinpoint terror targets and, in so doing, spotlighting vulnerabilities within those targets.

The government has a long history of experience using classified information to defend our nation. In fact, America has used such information in support of diplomacy. When a conflict arises, classified information plays a critical role in supporting military operations. However, the potency of classified information in the battle against terrorism becomes a liability when the battlefront shifts from the streets to the courtroom. The very factors that

---

* BA, University of Maryland; JD, Brigham Young University. Faculty Member, National Intelligence University. Mr. MacKay has previously served as an Assistant General Counsel at the Defense Intelligence Agency, and as the initial Legal Advisor to the Prosecutor for the Special Court for Sierra Leone. He has lectured at The Judge Advocate General's School, Utah State University, Utah Valley University, Georgetown University, the Catholic University of America, the Central Intelligence Agency, the Federal Bureau of Investigation, the Drug Enforcement Administration, the Joint Counterintelligence Training Academy, and the intelligence services of the Federal Republic of Germany, the Republic of Korea, the Republic of the Philippines, the Kingdom of Sweden, the Republic of Croatia, and Romania. The content of this article is the author's own, and does not reflect the position of the National Intelligence University, the Defense Intelligence Agency, or the Department of Defense.

1. Joshua, The Computer War Games (United Artists and Sherwood Productions 1983), directed by John Badham, starring Matthew Broderick, Ally Sheedy, and John Wood. Internet Movie Data Base (IMDB), last accessed Sept. 8, 2016, http://www.imdb.com/title/tt0086567/trivia?tab=qt&ref_=tt_trv_qu.

make classified information so valuable to our government operate to make this unique form of information problematic in the criminal trial of a terrorist.

This paper does not purport to offer a solution to the conundrum. Instead, it serves to highlight some considerations the government faces every time a criminal prosecution implicates classified information. The paper briefly examines the nature of classification, what can make information classified, and how the classification and declassification systems work. It then turns to the courtroom to examine the constitutional and pragmatic considerations involved in mounting a prosecution.

II. BACKGROUND

A. America's History with Great Britain and Her Courts

When the Constitutional Convention[2] of 1787 began its work in Philadelphia, its original task—revising the Articles of Confederation—was jettisoned in favor of building a national government that would work.[3] Experience during the Revolutionary War demonstrated the approach taken by the Articles was not tenable.[4] Rather, with the 1783 Treaty of Paris, that ended the war and recognized the newly-independent United States of America, the nation recognized it needed a governance structure that would reflect the issues that had fed the revolutionary flame.[5]

To limit the power of the American court system, the Grand Convention limited the reach of the judicial power to an actual case, and in doing so sharply reduced the likelihood of an activist bench.[6] To prevent what the colonists had perceived as an overreach, the Convention crafted a precise definition of treason and inserted that definition (the only crime so explicitly defined) into the Constitution.[7]

The First Amendment guaranteed the freedom to speak, assemble, worship, and petition the government for redress—all without penalty.[8] The Fourth Amendment inserted a warrant requirement, insisting upon specificity.[9] The British practice of the general warrant was banned by

---

2. Hereinafter "Grand Convention."
3. Richard R. Beeman, *The Constitutional Convention of 1787: A Revolution in Government*, NATIONAL CONSTITUTION CENTER (Sept. 27, 2017, 7:47 PM), https://constitutioncenter.org/interactive-constitution/white-pages/the-constitutional-convention-of-1787-a-revolution-in-government.
4. *See id.*
5. *Treaty of Paris*, HISTORY (Sept. 27, 2017, 7:48 PM), http://www.history.com/topics/american-revolution/treaty-of-paris.
6. *See* U.S. CONST. art. III, § 2.
7. *Id.* at §3.
8. *See* U.S. CONST. amend. I.
9. *See* U.S. CONST. amend. IV.

implication.[10] The Fifth Amendment precluded self-incrimination, a factor of the Star Chamber's "ex officio" oath which required a witness to truthfully answer all questions put to him, without the ability to remain silent.[11] No more would a witness be forced to either incriminate or perjure himself. Other Fifth Amendment provisions included the subpoena power, the right of confrontation, and the preclusion of double jeopardy.[12] The Sixth Amendment added the right of representation, along with a speedy and *public* trial.[13] Whatever the original utility of the Star Chamber, with its ability to deal with alleged malefactors amongst the English nobility, the closed and secret nature of the Chamber all too quickly led to abuse.[14] The newborn United States would have none of that.

B. The Clash of Concepts

Louis Brandeis, at the time a practicing attorney, penned a phrase regarding the dangers of secrecy when he wrote, "[p]ublicity is just commended as a remedy for social and industrial diseases. Sunlight is said to be the best of disinfectants; electric light the most efficient policeman."[15] Lord Hewart, writing in the British case, *R. v. Sussex Justices, Ex Parte McCarty*, described a situation (permissible under the law at the time) in which the clerk of the court hearing a criminal dangerous driving case was also working as a member of a firm pursing that same driver on a related civil claim.[16] The clerk retired with the justices, on the theory the learned solons of the law may have a fact question or two for their clerk.[17] In the event there were no such questions, and on appeal, the court conceded the clerk's sole participation in the justices' deliberation was a mute presence in chambers: he neither spoke, nor were his notes consulted.[18] Nevertheless, Lord Hewart overturned the verdict below, coining a phrase that still echoes today: "[I]t is not merely of some importance but is of fundamental importance that

10. Henry Farrell, *America's Founders Hated General Warrants. So Why Has the Government Resurrected Them*, THE WASHINGTON POST (Jun. 14, 2016) https://www.washingtonpost.com/news/monkey-cage/wp/2016/06/14/americas-founders-hated-general-warrants-so-why-has-the-government-resurrected-them/?utm_term=.b15cde895ebe.
11. U.S. CONST. amend. V; see also R.H. Helmholz, The Privilege Against Self Incrimination: Its Origins and Development 101 (1977).
12. *See* U.S. CONST. amend. V.
13. U.S. CONST. amend. VI.
14. Scott Horton, *Resurrecting the Star Chamber*, Harper's Magazine (Nov. 23, 2007, 9:08 AM) https://harpers.org/blog/2007/11/resurrecting-the-star-chamber/.
15. *See* Frederick A. Stokes, Other People's Money and How the Bankers Use It (2016).
16. *See* R. v. Sussex Justices, Ex parte McCarthy [1924] 1 KB 256, [1923] Eng. Rep. 233.
17. *Id.*
18. *Id.*

justice should not only be done, but should manifestly and undoubtedly be seen to be done."[19]

Implementing justice behind closed doors is not impossible, but maintaining the public's trust and confidence in its justice system cannot long survive darkness. In fact, at the time of the writing of this article, the current masthead of the *Washington Post* newspaper reads "Democracy Dies in Darkness."[20] Yet, the intelligence services of the world seek a totally different environment.

Speaking in the House of Commons in 1924, the British Foreign Secretary, Austen Chamberlain uttered, "It is of the essence of a Secret Service that it must be secret, and if you once begin disclosure it is perfectly obvious to me . . . that there is no longer any Secret Service and that you must do without it."[21]

While sounding like hyperbole to today's reader, at the time, the government of the United Kingdom simply did not admit that it had an intelligence service.[22] This is a position the government maintained through the 1980s.[23] In fact, Sir Michael Howard, a well-known British historian, bitingly commented in 1985, "so far as official government policy is concerned, the British security and intelligence services do not exist. Enemy agents are found under gooseberry bushes and intelligence is brought by the storks."[24]

The approach in the United States historically has focused more on protecting the activities and personnel of the assorted intelligence agencies

---

19. *Id*. at 259.

20. Paul Farhi, *The Washington Post's New Slogan Turns Out to be an Old Saying,* THE WASHINGTON POST (Feb. 24, 2017), https://www.washingtonpost.com/lifestyle/style/the-washington-posts-new-slogan-turns-out-to-be-an-old-saying/2017/02/23/cb199cda-fa02-11e6-be05-1a3817ac21a5_story.html?utm_term=.18d429676b9f.

21. *A Not-So-Secret Service*, TIME (Sept. 1, 1986), http://content.time.com/time/magazine/article/0,9171,962161,00.html.

22. Luke Jones, *The time when spy agencies officially didn't exist,* BBC NEWS (Nov. 8, 2014), http://www.bbc.com/news/magazine-29938135.

23. *See* Hew Dylan, Defence Intelligence and the Cold War: Britain's Joint Intelligence Bureau 1945–1964 1 (Oxford Univ. Press 2014).

24. *Id*. The British intelligence community is largely composed of the Secret Intelligence Service (SIS, unofficially known as MI-6), the UK counterpart to the Central Intelligence Agency; and the Government Communications Headquarters GCHQ), the UK counterpart to the National Security Agency, and the Security Service (also known as Ml-5), loosely the UK counterpart to the Federal Bureau of Investigation (the FBI has arrest powers, while the Security Service does not). Glen Greenwald, *Revealed: how US and UK spy agencies defeat internet privacy security*, The Guardian (Sept. 6, 2013 6:24 PM), https://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security; *See generally* Jonjo Robb, *The 'Intelligence Special Relationship' between Britain and the United States*, E-INT'L RELATIONS STUDENTS (June 15, 0214), http://www.e-ir.info/2014/06/15/the-intelligence-special-relationship-between-britain-and-the-united-states/.
The existence of SIS and GCHQ was officially confirmed for the first time in the Intelligence Services Act 1994. The Security Service has a public history tracing back to 1909, as a joint effort of the Admiralty and the War Office. *See* Jones, *supra* note 23.

than it has in trying to conceal the existence of the agencies themselves.[25] The Director of National Intelligence specifically, and by logical derivation of every other U.S. intelligence organization, is charged by statute with the protection of intelligence and methods.[26]

The result is a clash: democracies abhor secrecy, while secret services abhor sunlight. Yet, governments cannot survive without intelligence, and an intelligence service without some form of public accountability rapidly becomes a threat to the government it is established to serve. The challenge is to manage the tension between the competing needs of transparency and opacity.

III. ANALYSIS

A. The Nature of Classified Information

1. What is classified information?

Executive Order (hereinafter EO) 13,526 defines classified information as information the national defense requires "be maintained in confidence in order to protect our citizens, our democratic institutions, our homeland security, and our interactions with foreign nations."[27]

Classified information is the exclusive purview of the federal government.[28] While private sector individuals or entities may be afforded

25. *See* 50 U.S.C. § 403-4 (2012). The National Security Act of 1947 created, among other entities, the Central Intelligence Agency. CIA would later have its own enabling statute (50 U.S.C. §§ 403 et seq.). The Director of National Intelligence, with accompanying Office of the Director of National Intelligence, was created by the Intelligence Reform and Terrorism Prevention Act of 2004. Other intelligence entities are contained within assorted Cabinet departments (State, Justice, Defense, Treasury, Homeland Security) and have typically been established via a combination of secretarial decree and statutory provisions. For example, the National Security Agency, the Defense Intelligence Agency, and the National Geospatial-Intelligence Agency all exist with the Department of Defense. Each has a specific statutory exemption from the Freedom of Information Act for operational files, even though each organization was created by internal DoD directive.

26. *See* 50 U.S.C. § 403-l(i). In some cases, that injunction includes protecting the identities of employees of the intelligence agency, as well as the agency's size and budget.

27. *See* Exec. Order No. 13,526, 75 Fed. Reg. 707 (Dec. 29, 2009); *see also The President Executive Order 13526*, NATIONAL ARCHIVES SECURITY OVERSIGHT OFFICE (Sept. 26, 2017, 8:06 PM).

28. *See* Exec. Order No. 13,526, 75 Fed. Reg. 707 (Dec. 29, 2009). Section 1.1(2) describes classified information as owned by, produced by or for, or under the control of the United States Government. Information is "owned by" or "produced by" the federal government when it is created by a government entity. It may be "produced for" the federal government, such as when a private sector firm develops information or a tangible thing for the federal government. Examples would be Lockheed Martin's creation of the world's fastest airplane, the SR-71, and the creation of the world's first stealth aircraft, the F-117. Both airplanes were "tangible things" the existence of which was originally classified. Both airplanes contained subsystems (in the case of the SR-71, the propulsion system that generated still-classified speeds; in the case of the F-117, the technology that rendered the aircraft extremely difficult to detect on radar) containing "information" that was and remains classified. Information "under the control of" the federal government may have been provided to

access to classified information, ownership of that information always remains with the federal government.[29]

Classified information reflects an assessment of the risk to national security should the information be generally available. The more significant the risk, the higher the classification.[30]

The risk to national security assessment, per the Executive Order, cannot be based upon a perceived need to conceal violations of the law, inefficiency, or administrative error.[31] Nor can it be perceived to preclude embarrassment, to restrain competition, or to hinder dissemination of information that does not require protection based upon national security needs.[32] These restrictions are a direct reflection of the "Pentagon Papers" case, in which a 47-volume history of America's involvement in Vietnam was classified "Top Secret—Sensitive."[33] The history depicted a level of activity heretofore unknown to the American public. A researcher, opposed to the Vietnam War, with access to the history, made an unauthorized copy and provided it to the *New York Times*.[34] As the *Times* published extracts from the 47-volume history, it became clear that much of the material classified was marked to preclude embarrassment.[35] The resulting legal action was a resounding loss for the government. Modern classification criteria clearly reflect the "Pentagon Papers" experience.[36]

---

the United States by a foreign government, or an international organization, with the understanding that the U.S. government would protect that information at the same level as U.S. classified information. An example of information "under the control of" the federal government would be NATO classified information. The United States does not "own" that information, but by agreement with NATO would treat and protect that data as if it were US classified information. The only mention of what could be considered "classified information" in the Constitution is in Article l, Section 5: "Each House shall keep a Journal of its Proceedings, and from time to time publish the same, excepting such Parts as may in their Judgment require Secrecy."

29. Lockheed Martin designed and tested both the SR-71 and the F-117 for specific combat purposes. The designers required access to classified information in order to develop aircraft that could succeed in the known and anticipated threat environment.
30. If the unauthorized release of classified information would cause "exceptionally grave" damage to the national security, it is classified at the Top Secret level. The unauthorized release of information that would cause "serious damage" is classified at the Secret level, and the unauthorized release of information that would cause "damage" is classified at the Confidential level. *See* Exec. Order No. 13,526 § 1.2, 75 Fed. Reg. 707 (Dec 29, 2009).
31. Exec. Order No. 13526.
32. *See generally* Exec. Order No. 13,526 § 1.7, 75 Fed. Reg. 707, 710 (Dec. 29, 2009).
33. N.Y. Times Co. v. United States, 403 U.S. 713 (1971).
34. *Id.* at 714.
35. *Id.* at 723–24.
36. The issue before the Court was whether the government could enjoin further publication of the "Papers" by authority of 18 U.S.C. § 793. The Court construed § 793 narrowly, and ultimately ruled that the government had not met its very heavy burden and permitted publication to continue. Unaddressed by the Court was the possibility of post-publication prosecution. The government, perhaps realizing that any such prosecution would logically trigger a challenge to the classifications applied, elected not to pursue the Times. The government was able to identify the individual who provided the "Papers" to the Times, and prosecuted him. However, the White House's attempt to

Classification is appropriate if the unauthorized disclosure of information would cause "damage" to the national security, and that information pertains to any of the following categories: (1) military plans, weapons systems, or operations; (2) foreign government information; (3) intelligence activities (including covert action); (4) intelligence sources, methods, or cryptology; (5) foreign relations or foreign activities of the United States, including confidential sources; (6) scientific, technical, or economic matters relating to the national security United States Government programs for safeguarding nuclear materials or facilities; (7) vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to the national security; or (8) the development, production, or use of weapons of mass destruction.[37]

2. Who can classify information?

Authority to classify information exists in two, unequally sized, populations. The first, smallest yet most important, are the "original classification authorities." These are those individuals identified by the President as authorized to determine whether information should be classified and, if so, at what level.[38] Within broad guidelines, designed original classification authorities typically may delegate that authority within their own organizations.[39]

As a matter of practicality, original classification authorities direct the creation of classification guides. These guides take the classification concepts of Executive Order 13,526 and apply them within the context of the classifier's organization. The resulting guides are used by the largest population, those who apply classifications derived from the guide. Those who apply derived classifications are known as derivative classification

---

ensure conviction by burglarizing the defendant's psychiatrist's office, and providing the defendant's medical file to the prosecution, sufficiently outraged the bench that a mistrial with prejudice was declared.

37. *See* Exec. Order No. 13,526 § 1.4, 75 Fed. Reg. 707, 707 (Dec. 29, 2009).

38. *See id.* This identifies the President and Vice President as original classification authorities at all classification levels. The listing of additional original classification authorities is published in the Federal Register. The current list designates the White House chief of staff and national security advisor; the Attorney General; the secretaries of State, Treasury, Defense, Energy, Homeland Security; the Director of National Intelligence; the secretaries of the military services; the Director of the Central Intelligence Agency and the Administrator of the National Aeronautics & Space Administration as original Top Secret classification authorities. In that role, these individuals may also classify information at lower classification levels. At the Secret level, the secretaries of Agriculture, Commerce, Health & Human Services, Transportation, and the administrator of the Environmental Protection Agency are original classification authorities. *See* Federal Register, Vol. 75 No. 2, January 5, 2010.

39. *See* Exec. Order No. 13,526 § 1.3(c)(1), 75 Fed. Reg. 707, 708 (Dec. 29, 2009) (One of the broad guidelines is that delegations of original classification authority "shall be limited to the minimum required . . .").

authorities.[40] These derivative classification authorities produce the overwhelming majority of classified information.

3. Who can declassify information?

The authority to classify a document carries with it implicit authority to declassify that same document. As a general rule, declassification authority ends at the organization's edge; the Central Intelligence Agency has no authority to declassify a Department of Defense document, for example.

There are a limited number of exceptions to this rule. The President, as the ultimate classification authority, is also the ultimate declassification authority. The Director of National Intelligence has the authority to declassify intelligence "relating to intelligence sources, methods, or activities," in consultation with that information's original classification authority.[41]

4. What makes information classified?

Information is classified based on a combination of factors: content, the extent to which the information may identify U.S. interest in the topic, and (in the intelligence world) on the means of its acquisition.

This combined approach can explain the occasional oddity of having information that, by itself, might be unclassified yet still bear classification markings. [An example would be a publication intended for internal use only, such as the Kremlin's internal telephone directory.] While this would technically not be "classified information," per se, the directory could still be marked as classified to protect how the United States obtained it. Was it provided by an agent inside the Kremlin? Was a clever visitor able to purloin a copy without being detected? Did a clerk erroneously ship a copy to a person willing to give it to us? If classifying the method of acquisition is necessary, the classification will extend to the directory as well (on the theory that the presence of the directory would tend to identify possible means of acquisition).

---

40. *See generally* Exec. Order No. 13,526 § 2, 75 Fed. Reg. 707 (Dec. 29, 2009).

41. Exec. Order No. 13,526 § 2, 75 Fed. Reg. 707 (Dec. 29, 2009) ("methods, and activities. The Director . . . may, with respect to the Intelligence Community, after consultation with the head of the originating Intelligence Community element or department, declassify, downgrade, or direct the declassification or downgrading of information or intelligence relating to intelligence sources, methods, or activities."). The Director may only delegate this authority to the Principal Deputy Director of National Intelligence. This provision allows the DNI, as the nation's chief intelligence officer, to mandate declassification of information developed by the Intelligence Community. There is much classified information *not* so developed, and the DNI's authority to declassify that information is non-existent.

Another example comes from the Penkovsky espionage case of the early 1960s.[42] Colonel Oleg Penkovsky volunteered to work for Western intelligence.[43] Run jointly by the Central Intelligence Agency and the United Kingdom's Secret Intelligence Service, Penkovsky was asked to obtain a copy of the secret version of a Soviet military journal, *Military Thought.*[44] The unclassified version of that journal was available in the West.[45] Penkovsky, bemused, asked his handlers if they would want a copy of the top secret version of the same journal.[46] Possession of the unclassified version of *Military Thought* would not be remarkable, as many Western entities had annual subscriptions. Our Intelligence Community would have no reason to mark this version as classified. Possession of the secret version, had the Soviet Union become aware, would immediately focus suspicion on those organizations within the USSR to which that version had been sent. Identifying the source who had provided this version to the West would have been much easier, with severe potential consequences for the source if caught.

Logically, any copy of the secret version of *Military Thought* in U.S. possession would be marked "SECRET"—not because the U.S. was honoring the Soviet classification, but because Soviet knowledge of U.S. possession of the document could cause serious damage to our national security.[47]

The top-secret version, new at the time, was only distributed to "officers, Admirals, and Generals of the Soviet Army."[48] Compromise of the U.S. possession of any of these versions would have immediately focused intense scrutiny upon a much smaller population, with potentially catastrophic consequences for the source. A source positioned to provide this level of information would logically be able to provide other data, likely of equal significance, which the U.S. would likely rely upon. Compromising that source, by revealing possession of the top-secret version of *Military Thought*, would likely have

42. DAVID E. HOFFMAN, THE BILLION DOLLAR SPY: A TRUE STORY OF COLD WAR ESPIONAGE AND BETRayal 12–14 (2015).

43. *Id*.

44. *Id*. at 15.

45. MILITARY THOUGHT JOURNAL, CENT. INTELLIGENCE AGENCY (2017), https://www.cia.gov/library/readingroom/keyword/military-thought-journal.

46. *See* JEREMY DUNS, DEAD DROP 78–79 (2013).

47. There is some debate in the Intelligence Community whether the appropriate classification should be derived primarily from the risk to the intelligence source, and not the potential damage to U.S. national security interests, should the source be compromised. To at least some extent, the discussion is academic, because as a practical matter the sources facing the gravest risks tend to be providing information of the greatest value. Therefore, whether the classification is derived from "risk-to-source" or "risk-to-nation," the result is typically the same.

48. Duns, *supra* note 46, at 79.

caused "exceptionally grave damage" to the U.S. and as a result would trigger the Top-Secret classification.[49]

The Penkovsky case illustrates classification in the human intelligence (HUMINT) arena, in which intelligence services rely upon human beings to provide information.[50] The world of signals intelligence (SIGINT) is another source of information, and has been historically lucrative.[51] The classic example of SIGINT effectiveness was the success against the German (ULTRA) and Japanese (MAGIC) encryption systems used in WWII.[52]

In the aftermath of the Pearl Harbor attack, the U.S. military's capabilities in the Pacific were a fraction of their previous strength. What had been a battleship- and heavy cruiser-dominated fleet, no longer existed.[53] The previous naval warfare strategy based around major surface combatants (battleships and cruisers), supported by carrier-based aviation and submarines, became a necessity of submarine-centric strategy (with use of carrier-based aviation if and when a significant surface target could be located). There is some debate in the Intelligence Community whether the appropriate classification should be derived primarily from the risk to the intelligence source should the source be compromised, or the potential damage to U.S. national security interests. To at least some extent, the discussion is academic, because, as a practical matter, the sources which faced the gravest risks tended to provide information of the greatest value. Therefore, whether the classification is

---

49. Arvin S. Quist, *Security Classification of Information*, OAK RIDGE NATIONAL LABORATORY, https://fas.org/sgp/library/quist2/chap_7.html.

50. CENTRAL INTELLIGENCE AGENCY, *Intelligence: Human Intelligence* (Oct. 21, 2010, 11:30 AM), https://www.cia.gov/news-information/featured-story-archive/2010-featured-story-archive/intelligence-human-intelligence.html.

51. David A. Hatch, *ENIGMA and PURPLE: How the Allies Broke German and Japanese Codes During the War*, https://www.usna.edu/Users/math/wdj/_files/documents/Cryptoday/hatch_purple.pdf (last visited Sept. 19, 2017).

52. *Id.*

53. The Navy complement in Pearl Harbor as of December 7, 1941 could be divided in two: power-projection platforms (battleships, cruisers, destroyers, submarines, aircraft carriers, etc.), and defensive or support platforms (minesweepers, tenders, oilers, tugs, etc.). In the power-projection category, 16 of the 50 ships were severely damaged or sunk. The attack concentrated on major surface combatants (battleships and cruisers), and was devastatingly effective. All of the nine battleships present were severely damaged or sunk, although six would rejoin the fleet later in the war. Five of the eight cruisers were damaged to some extent. Most of the destroyers, and all of the submarines, survived. The overwhelming majority of the defensive/support platforms survived as well. The Pacific Fleet possessed a total of three aircraft carriers, all of which were at sea on December 7, 1941. *See List of United States Navy ships present at Pearl Harbor, December 7, l941*, WIKIPEDIA, https://en.wikipedia.org/wiki/List_of_United_States_Navy_ships_present_at_Pearl_Harbor,_December_7,_1941 (last visited Apr. 28, 2016).

derived from "risk-to-source" or "risk-to-nation," the result is typically the same.

The Japanese strategy, based on Admiral Yamamoto's assessment of U.S. capabilities, was to strike hard and unexpectedly destroy America's power-projection capability in the Pacific: the U.S. Navy.[54] The Pearl Harbor attack essentially destroyed America's surface warfare capability in the Pacific.[55] Yamamoto recognized the American carrier force was a threat, and designed an attack on Midway Island[56] to destroy the remnant of America's Pacific Fleet and force peace on Japan's terms.[57]

Yamamoto did not anticipate the capabilities of U.S. SIGINT. Navy cryptographers, having achieved a level of success against the Japanese JN-25 code, were able to advise Admiral Nimitz that Japan was preparing to move against Midway, and provided him the date of the attack.[58] This knowledge allowed Nimitz to place his three carriers where they could do the most good against a significantly larger Japanese force.[59] Armed with information, a good deal of luck, and perseverance Nimitz soundly defeated Yamamoto, sinking all of his carriers, one of his heavy cruisers, and killing 2,500 of his sailors.[60] The U.S. lost the carrier YORKTOWN, the destroyer HAMMAN, and 307 sailors.[61] The Battle of Midway was the turning point

---

54. *See* Peter D. Antill et al., *The Battle of Midway: Turning Point in the Pacific Campaign 3-7 June 1942*, HIST. OF WAR, http://www.historyofwar.org/articles/battles_midwaylong.html (last visited Sept. 20, 2017).
55. According the History.com, "the Japanese had failed to cripple the Pacific Fleet." *Pearl Harbor*, HISTORY, http://www.history.com/topics/world-war-ii/pearl-harbor (last visited Sept. 30, 2017).
56. Midway Atoll is located 1,120 miles north-west of the Hawaiian Island chain. *The Battle of Midway—Historical Overview*, THE PAC. WAR HIST. SOC'Y, http://www.pacificwar.org.au/Midway/MidwayOverview.html (last visited Sept. 30, 2017).
57. *Id.*
58. *Id.*
59. This chart provides some insights into the force imbalance at the Battle of Midway:

Vessel Type:	Imperial Japanese Navy forces	U.S. Navy Forces
Aircraft Carriers:	4	3
Light Aircraft Carriers:	2	0
Seaplane Tenders:	3	0
Battleships:	11	0
Heavy Cruisers:	10	7
Light Cruisers:	6	1
Destroyers:	46	20
Submarines:	16	19

See Midway Order of Battle, WIKIPEDIA, https://en.wikipedia.org/wiki/Midway order of battle (last visited Apr. 28, 2017).

60. *List of United States Navy ships present at Pearl Harbor, December 7, l941*, WIKIPEDIA, https://en.wikipedia.org/wiki/List_of_United_States_Navy_ships_present_at_Pearl_Harbor,_December_7,_1941 (last visited Apr. 28, 2016).
61. *Id.*

in the naval war in the Pacific.[62] Never again would the Japanese Navy sail with impunity. It remained on a defensive footing for the balance of the war.[63]

5. How is classified information protected?

First, classified information is clearly marked to indicate the level of classification and any restrictions on its handling.[64]

Second, classified information is stored within facilities specifically designed for that purpose.[65] Low-level classified information might be stored in an approved security container in an otherwise open office; high-level classified information would typically be stored in a purpose-built facility.[66]

Third, classified information is only provided to those persons whose personal backgrounds have been investigated and found to be suitable persons in whom the government can repose trust and confidence to protect classified information.[67]

---

62. *Id.*

63. *See generally Battle of Midway ends*, HISTORY, http://www.history.com/this-day-in-history/battle-of-midway-ends (last visited Apr. 28, 2017).

64. 50 U.S.C. § 3126 (2012). There is a taxonomy-driven manual that describes how pages, and individual paragraphs, are to be marked. While that unclassified manual has not been cleared for public release, its intent is to make obvious to the reader which portion, of which document, requires which form of protection. This precision in marking makes use of the classified information easier, and reduces the risk of inadvertent release. An example of "restricted handling" would be information received from a foreign government, or an international organization. While the United States would be authorized to hold, and to use, that information, the originating government would typically reserve the right to control its onward dissemination. Any such document held by the United States would logically bear a "restricted handling" marking indicating that onward dissemination would require the originating government's or organization's permission.

65. *See* NAT. SEC. AGENCY, 440-3-H, NATIONAL SECURITY INFORMATION HANDBOOK (1991), https://www2.usgs.gov/usgs-manual/handbook/hb/440-3-h.html#chapter8.

66. *See* NAT. SEC. AGENCY, 440-3-H, NATIONAL SECURITY INFORMATION HANDBOOK (1991), https://www2.usgs.gov/usgs-manual/handbook/hb/440-3-h.html#chapter8_2. As one might expect, access to a purpose-built facility would typically be restricted to those whose duties require access. As a general rule, access to the facility would require a security clearance equal to the highest level of information stored in that facility. NAT. SEC. AGENCY, 440-3-H, NATIONAL SECURITY INFORMATION HANDBOOK (1991), https://www2.usgs.gov/usgs-manual/handbook/hb/440-3-h.html#chapter14_3.

67. NAT. SEC. AGENCY, 440-3-H, NATIONAL SECURITY INFORMATION HANDBOOK (1991), https://www2.usgs.gov/usgs-manual/handbook/hb/440-3-h.html#chapter3_1. The level of security clearance required dictates the depth and scope of the background investigation. The highest level security clearances require a background investigation that can take as much as a year to complete. Some clearances also require successful completion of a polygraph examination.

Fourth, classified information is only provided to those individuals whose duties clearly require that access.[68] Mere possession of a security clearance is not sufficient.[69]

6. How is classified information used?

The primary purpose of information is to provide decision makers with decision advantage. Classified information is particularly valuable, as it has the potential to provide depth, breadth, or detail not publicly available. Such granularity of detail allows decision makers the ability to produce nuanced decisions to advance the nation's interests.

One continuing issue with intelligence information is the conundrum of risk vs. gain. The information any nation needs the most is often the information that is most vigorously protected by its owner. If access to that information can be gained at all, the recipient must also protect it vigorously; if the information's owner learns of its loss, the utility of that information in the recipient's hands is questionable. The result is that the most sought information is the hardest to use without revealing it is in the recipient's possession.

In battlefield situations, the value of intelligence information can be fleeting—the location(s) of enemies or their intentions, and can change very rapidly. If the value is fleeting, the need to protect possession of that information is also likely to be fleeting; in like manner, the shorter the "shelf life" of intelligence information, the greater the ability to make aggressive use of that information.

However, in a national-strategic environment, the shelf life of intelligence information could be measured in years, and perhaps even decades. In those cases, decisions about how, and when, to make use of intelligence information takes on a different set of considerations.

---

68. 46 C.F.R. § 503.59(d)(2) (2014).

69. *Id.* §§ 503.59(d)(1)-(2). While there are only three clearance levels (corresponding to the three levels of security classification: Confidential, Secret, and Top Secret), there are multiple "compartments" to restrict access to certain categories of information. For example, the President's helicopter crew requires a Top Secret security clearance, but the information it receives is that relevant to flight planning, flight safety, and the President's security. An intelligence analyst may also have a Top Secret security clearance, but have no access to Presidential security information. The principle is akin to that used in naval vessels: all crew are on-board, but watertight doors secure individual compartments on the ship, so that if one is penetrated, the damage can be contained and prevent the ship from sinking.

B. Use of Classified Information in Trial

1. How is classified information used in trial?

The first consideration, always implicated when the question of the use of classified information in trial arises, is "whether the use of classified information is in the best interests of the United States?" Remember, in the United States, there is a statutory obligation to protect intelligence sources and methods.[70] "Intelligence information" is the result of a source, or a method, or some combination thereof; it itself is neither a "source" nor a "method." Therefore, the starting logical position is that the information (the "intelligence") sought for release may be released without offending the statute's requirement of protection.

However, that theoretical starting position immediately collides with analysis of factors regarding United States best interests, use of information as evidence, and the Director of National Intelligence's statutory duties. The "harm" question should always come first, as the Director of National Intelligence has a statutory duty to protect intelligence sources and methods.[71] Many collection systems represent not only a great deal of money, but time and effort in their development.[72] The product of those systems often requires specialist training and experience to convert the product into data useable by humans.[73] Exposure of the collection, processing, or analytic methods involved could hinder, if not destroy, the future utility of those methods.

Also, an intelligence collection is designed to provide information, not "evidence" capable of withstanding cross-examination as to provenance, accuracy, and relevance.[74] Thus, the inquiry should consider any alternative methods which could obtain the same evidence.[75] For example, satellite images, images from military drones, and images from a law enforcement drone are all "pictures." The product from the law enforcement drone is likely going to be easier to use in court, as it was collected by a law enforcement officer familiar with evidentiary and

70. NAT. SEC. AGENCY, 440-3-H, NATIONAL SECURITY INFORMATION HANDBOOK (1991), https://www2.usgs.gov/usgs-manual/handbook/hb/440-3-h.html#chapter10_2.

71. *See* 50 U.S.C. § 3024(i)(1) (2012).

72. 2016 ISOO Ann. Rep. 19, https://www.archives.gov/files/isoo/reports/2016-annual-report.pdf.

73. *See* U.S. Dept. of Justice, Audit Report 05-32, Processing Classified Information on Portable Computers in the Department of Justice (2005), https://oig.justice.gov/reports/plus/a0532/final.pdf.

74. *See* Patrick Dunleavy, *Intelligence vs. Evidence Gathering: Knowing the Difference*, THE INVESTIGATIVE PROJECT ON TERRORISM (Aug. 29, 2011) https://www.investigativeproject.org/3132/intelligence-vs-evidence-gathering-knowing.

75. Steven Aftergood, *A Tutorial on the Classified Information Procedures Act*, FED'N OF AM. SCIENTISTS (May 10, 2010), https://fas.org/blogs/secrecy/2010/05/cipa_tutorial/.

chain-of-custody requirements. Such matters are largely unaddressed by intelligence officers, as they are not relevant to the intelligence craft.[76]

Thus, "whether the information sought can, in fact, be released without harming sources or methods" hinges on the answers to at least the following questions:

- What would the harm to the United States be, if the intelligence information was revealed in open court? Conversely, what benefit would accrue to the United States if that intelligence information was used?
- How did the United States come into possession of the information in question? Was it unilateral collection? Collection via some technical system, or from a human? Did a foreign government, or an international organization, provide the information?
- Can the information be used without compromising the collection method(s) involved?
- Does the information meet minimum evidentiary standards?
- If not, is there an alternative collection method, not linked to intelligence, that could provide substantially the same information?

All of these factors, construed and analyzed as a whole, lead to the decision of whether or not use of classified information at trial is in the best interests of the United States. However, there are additional considerations in play.

2. What is the venue?

As a matter of policy, the United States does not use classified information in state criminal trials.[77] Classified information is the property of the United States, or at a minimum is under federal control.[78] The only trial venue in which the United States would normally use classified information is the federal court system.[79] In the unlikely event a state criminal trial would somehow implicate classified information, the federal government would attempt to intervene and remove the case to federal court.[80]

---

76. *See generally* Milena Sterio, The Covert Use of Drones: How Secrecy Undermines Oversight and Accountability, 8 ALB. GOV'T L. REV. 129, 164 (2015); Timothy M. Ravich, Courts in the Drone Age, 42 N. KY. L. REV. 161 (2015).
77. Edward C. Liu & Todd Garvey, Cong. Research Serv., R41742, Protecting Classified Information and the Rights of Criminal Defendants: The Classified Information Procedures Act 9 (2012), https://fas.org/sgp/crs/secrecy/R41742.pdf.
78. *See* 18 U.S.C. § 1924(c) (2012).
79. 18 U.S.C. §§ 1-16(2012).
80. *See* 28 U.S.C. § 1442 (a)(1), (d)(1) (2012).

Federal judges do not hold security clearances.[81] They are afforded access to classified information as a function of their positions, and the investigation is conducted as a routine component of the judicial nomination process.[82] The Executive Branch has taken the position that comity precludes additional investigation of federal judges.[83] The staffs of federal courts, on the other hand, are subject to the same investigative standards and requirements as any other federal employee whose duties may require access to classified information.[84] If a federal criminal case requires the use of classified information, which is not uncommon in terrorist and espionage cases, security arrangements are developed on an as-needed basis to support the trial while protecting the classified information involved.[85]

The Classified Information Procedures Act is a specific federal statute which governs the procedures used when classified information is intended for use in criminal trials.[86] That statute addresses policy—in the sense of whether or not the classified information sought for use at trial will actually be used—by putting the federal government to an election.[87] After assorted procedural steps designed to protect both the defendant's right to defend himself and the government's need to protect classified information, the bench ultimately decides whether any of the lesser methods provided for by statute preserves the defendant's rights.[88] If the bench concludes that they do not and the government cannot or will not

---

81. DEPT. OF JUSTICE, UNITED STATES ATTORNEYS' MANUAL: CRIMINAL RESOURCE MANUAL 2054 (1997). https://www.justice.gov/usam/criminal-resource-manual-2054-synopsis-classified-information-procedures-act-cipa.

82. *Id*.

83. Liu, *supra* note 81.

84. Criminal Resource Manual, *supra* note 89.

85. Robert Timothy Reagan, Keeping Government Secrets: A Pocket Guide for Judges on the State-Secrets Privilege, the Classified Information Procedures Act, and Court Security Officers 19 (Fed. Jud. Ctr., 2007), https://fas.org/sgp/jud/judges.pdf. The Foreign Intelligence Surveillance Court has a purpose-built facility designed to accommodate the classified information it is presented. All other federal courts have varying degrees of secure information handling and storage capability. The matter is one normally addressed by the Department of Justice (directly, or via the local United States Attorney's office), the US Marshal's Service (responsible for federal courtroom security), and the proponent for the classified information involved. *See* Brian Palmer, *Do Judges Get to Look at Classified Documents?* Slate (Jun. 11, 2009), http://www.slate.com/articles/news_and_politics/explainer/2009/06/do_judges_get_to_look_at_classified_documents.html. *See also* U.S. Foreign Intelligence Surveillance Court Rules of Procedure (2010).

86. Classified Information Procedures Act, 18 U.S.C. app. 3 (2012). There is a separate, common-law based evidentiary privilege (the State Secrets privilege) available in civil suits. To be applicable, unless the United States is already a party to the action, it must be given leave to intervene. Once an intervenor, there must be a formal claim of privilege made by the head of the department with control over the matter, after actual, personal review of the material(s) for which privilege is claimed. Once the claim is made, the bench determines if the circumstances support the claim of privilege. *See* United States v. Reynolds, 345 U.S. 1, 7–8 (1953).

87. 18 U.S.C. app. 3, § 6 (2012).

88. *Id*. § 6(c).

make the classified information available, remedies available to the bench range from "dismissing specified counts of the indictment or information; finding against the United States on any issue as to which the excluded classified information relates; or striking or precluding all or part of the testimony of a witness."[89]

The international arena is more challenging. Unlike the domestic federal environment, which the Executive Branch can maintain a high level of control over the classified information desired for use in trial,[90] the international environment is beyond the control of any national government.

Initially, the same analysis takes place: is revelation of the classified information in the best interests of the United States? What would the harm or benefit be to the United States if intelligence information was revealed in open court? Is the means of intelligence information acquisition one that can be revealed without undue harm? Will use of the information compromise that collection method? Does the information meet the admissibility standard for use in the international tribunal? Not all tribunals use the same evidentiary standards; that which is permissible in one may not be permissible in another.[91]

Assuming all these hurdles have been cleared, which a significant assumption, there is a final statutory hurdle to surmount. No U.S. classified information may be provided to the United Nations, or any of its affiliated organizations, unless the President certifies to the relevant committees of Congress that the Director of National Intelligence, working with the Secretaries of State and Defense, has established mechanisms and procedures to protect any information to be released.[92]

---

89. *Id.* § 6(e)(2)(A)-(C).

90. *See* 50 U.S.C. § 3002 (2012).

91. The International Criminal Tribunal for the Fonner Yugoslavia (lCTY) and its counterpart for Rwanda (ICTR) had no rule against hearsay, a staple of the US court systems. *See* Rodney Dixon et al., Archbold International Criminal Courts: Practice, Procedure and Evidence 263 (Sir Adrian Fulford ed., Sweet & Maxwell 3d ed. 2009). On the other hand, the Special Court for Sierra Leone, mindful of the sometimes casual approach to human rights in Africa, adopted a rule barring admission of evidence "if its admission would bring the administration of justice into serious disrepute." *See* SCSL R. P. Evid. 95 (S. Afr.) (amended Mar. 7, 2003).

92. *See* 50 U.S.C. § 3042 (2012). There is a waiver provision, allowing the President to notify the appropriate committees of the Congress that provision of such information (presumably, in the absence of such procedures) is in the national security interests of the United States. While not explicitly stated, the assumption is that the waiver provision permits POTUS to act in an in extremis situation, such as providing US intelligence to a UN-sponsored hostage rescue force when time is of the essence. Note also that the statute does not specify which are the "appropriate" committees of the Congress. At a minimum, one would presume the House and Senate intelligence and foreign relations committees; since Defense is mentioned in the statute, the House and Senate armed services committees would seem logical as well.

Direct support of international criminal trials is not common, but it has happened.[93] One classic example is CIA's support of the trial of those accused of bombing Pan American World Airways flight 103, as detailed below.[94]

"On December 21, 1988, Pan American flight 103, a Boeing 747, took off from London, bound for New York City.[95] As it was climbing on its northerly flight path, it exploded over the town of Lockerbie in the Dumfries and Galloway region of southwest Scotland.[96] In all, 270 people from twenty-one countries died, including all 259 passengers and crewmembers plus eleven people on the ground in Lockerbie."[97]

The investigation of the bombing "was a jigsaw-puzzle assembly by many cooperating law-enforcement, intelligence, and legal personnel from numerous countries."[98] This collaborative effort included a CIA electronics expert who uncovered a key piece of evidence in 1989 from a piece of scorched shirt that was discovered to contain a fragment of a circuit that "had fused into the shirt's polyester fabric" from the heat of the explosion.[99]

The Scots photographed the circuit-board fragment and gave the photo to the FBI, who passed a copy to the CIA.[100] At the CIA, a Directorate of Science & Technology (DS&T) electronics expert observed two things he had seen before—a timer from an earlier Libyan terrorist attack.[101] Further analysis confirmed the fragment exactly matched part of a timer circuit manufactured specifically for the Libyans.[102]

In the Netherlands, a Scottish court presided over the two accused Libyans. The DS&T officer testified, but protected his identity through disguise, an alias, and alteration of his voice. The Libyans relied on the defense that the PLFP-GC bombed Pan Am 103, thus the expert's testimony was critical to rebut that theory.[103]

---

93. *See United States and the International Criminal Court*, WIKIPEDIA, https://en.wikipedia.org/wiki/United_States_and_the_International_Criminal_Court (last visited Sept. 24, 2017).
94. *CIA's Role in the Pan Am 103 Investigation and Trial (U)*, CENT. INTELLIGENCE AGENCY (Feb. 8, 2007, 1:08 PM), https://www.cia.gov/library/readingroom/docs/DOC_0001407030.pdf.
95. *Terrorist Bombing of Pan Am Flight 103*, Posted to *CIA Museum*, CIA, https://www.cia.gov/about-cia/cia-museum/experience-the-collection/text-version/stories/terrorist-bombing-of-pan-am-flight-103.html (last updated Nov. 21, 2012, 8:28 AM).
96. *Id.*
97. *Id.*
98. *Id.*
99. *Id.*
100. *Id.*
101. *Id.*
102. *Id.*
103. *Id.*

Forensic experts seek justice after an incident, whereas CIA experts work in the shadows to prevent the instance before it happens.[104] CIA employees are experts "in weapons, ordnance, electronics, and other field work."[105] Due to the CIA experts' requirement for anonymity, not many know their contributions to combat terrorism.[106]

The CIA expert's testimony, identifying the circuit-board fragment, was pivotal in the conviction of one accused Libyan terrorist.[107]

While the use of a CIA officer in the Pan Am 103 trial was successful (on two counts: the relevant evidence was presented in a manner acceptable to all parties, without compromising US intelligence sources, methods, or personnel; and a conviction was obtained), as a matter of practicality, the preferred approach in the international arena is for nations, including the United States, to provide classified information for "lead development purposes" only.[108] There is no intent to use the information at trial, rather, the information provided, typically ex parte to the prosecutorial staff, is designed to stimulate investigation along paths that, hopefully, will lead to the discovery of admissible evidence using means not involving foreign intelligence assets or capabilities.[109]

An example of this approach comes from the Rules of Procedure and Evidence used at the International Tribunal for the Former Yugoslavia. Rule 70 reads, in relevant part:

> (B) If the Prosecutor is in possession of information which has been provided to the Prosecutor on a confidential basis and which has been used solely for the purpose of generating new evidence, that initial information and its origin shall not be disclosed by the Prosecutor without the consent of the person or entity providing the initial information and shall in any event not be given in evidence without prior disclosure to the accused.
>
> (C) If, after obtaining the consent of the person or entity providing information under this rule, the Prosecutor elects to present as evidence any testimony, document or other material so provided, the Trial Chamber, notwithstanding Rule 98 [power of the court to order either party to produce additional

104. *Id.*
105. *Id.*
106. *Id.*
107. *Id.*
108. Rebecca Hughes Parker, *Anti-Money Laundering*, THE FCPA REPORT, Feb. 6, 2013, https://www.clearygottlieb.com/~/media/cgsh/files/publication-pdfs/former-fincen-director-james-h-freis-jr-discusses-the-intersection-between-anti-money-laundering-and-anti-corruption-law-part-one-of-two.pdf.
109. *Id.*

> evidence and summon witnesses], may not order either party to produce additional evidence received from the person or entity providing the initial information, nor may the Trial Chamber for the purpose of obtaining such additional evidence itself summon that person or a representative of that entity as a witness or order their attendance. A Trial chamber may not use its power to order the attendance of witnesses or to require production of documents in order to compel the production of such additional evidence.
>
> (D) If the Prosecutor calls a witness to introduce in evidence any information provided under this Rule, the Trial Chamber may not compel that witness to answer any question relating to the information or its origin, if the witness declines to answer on grounds of confidentiality.
>
> (E) The right of the accused to challenge the evidence presented by the Prosecution shall remain unaffected subject only to the limitations contained in Sub Rules (C) & (D).

The author's personal experience reflects the preference for provision of intelligence information for lead generation purposes only. While serving as the Legal Advisor to the Prosecutor of the Special Court for Sierra Leone, I also served as the Prosecutor's intelligence officer, charged with developing and maintaining intelligence relationships with those nations willing to share information with the Special Court. During my service, without exception, those nations willing to provide information did so on a "lead generation" basis only. One nation was willing to provide actual copies of documents, which I refused to receive on the theory that I could best protect their content by ensuring that the documents never entered the Special Court compound. Any information relevant to the Court's investigative or prosecutorial activities could be, and was, stripped of any identifying characteristics and then provided, orally, to the Chief of Prosecutions or Chief of Investigations for their use.[110] To the best of my knowledge, the information provided was used by those two offices without ever compromising from whence the original information came. I, as a matter of practice, *never* revealed the identity of the organization or entity that provided it.

110. *See Sanitization (classified information)*, WIKIPEDIA, https://en.wikipedia.org/wiki/Sanitization_(classified_information) (last visited Dec. 21, 2016) (The process of stripping intelligence information of data that would tend to identify its sourcing, or its method of collection, is called "sanitizing").

IV. THE CURRENT STATE

It would be convenient to be able to state that the United States has been able to develop a consistent, predictable, rapid system under which classified information of potential evidentiary use in a criminal trial can be provided, securely, to the parties involved without compromising intelligence sources and methods. In a land populated by wizards, dragons, and magic wands, that may be possible someday, but that is not the world in which we live.

When Louis Brandeis penned his famous "sunlight is the best disinfectant; electric light the most efficient policeman" line, the world's first mass-produced automobile had been in production for five years.[111] Today, Google is testing driverless cars.[112] In 1894, Marconi developed wireless telegraphy, and is credited with saving 700 of the Titanic's victims.[113] Today, most Americans carry in pocket or purse a device that will allow them to make voice calls to any place on the planet, and access the Internet from a bus stop. The twentieth century saw man move from being Earth-bound, to heavier-than-air flight, to transcontinental, intercontinental, and finally space travel. Who knows what developments will come next?

With each new technology development, the intelligence organizations of the world will try to find a way to use that development to produce intelligence information for the advantage of their decision-makers. The techniques, opportunities, and vulnerabilities that could be used to produce this information are impossible to predict.

In addition, people are unpredictable. The Soviet Union believed that Oleg Penkovsky was one of the anointed ones, destined for a position of prominence and fame in the Soviet hierarchy. They learned that he, in fact, was disaffected, and proved simultaneously to be an extraordinary risk to the USSR at precisely the time he was of extraordinary value to the West.[114] The CIA reposed great trust and confidence in Aldrich Ames, and he repaid it with treachery that cost incalculable amounts of money

---

111. Brandeis' line, contained in a serialized chapter from what would become "Other People's Money and How Bankers Use It," was published in 1914. The Model T went into production in 1908. *See Our Story*, FORD, https://corporate.ford.com/history.html.

112. *Google's Driverless Cars Make Progress*, BBC (Feb. 2, 2017), http://www.bbc.com/news/technology-38839071.

113. Gerard Hannan, *19th Century European Broadcasting*, IRISH MEDIA MAN, https://irishmediaman.wordpress.com/category/european-history/.

114. *The Capture and Execution of Colonel Penkovsky, 1963*, CENT. INTELLIGENCE AGENCY (last updated Apr. 30, 2013, 12:35 PM), https://www.cia.gov/news-information/featured-story-archive/2010-featured-story-archive/colonel-penkovsky.html.

in destroyed intelligence collection systems, and the loss of multiple human lives.[115]

Each proposal to use classified information in a criminal trial, whether it be terrorist, espionage, or some other matter, will have to be weighed on a case-by-case basis. There is not, nor can there be, a precise formula that will permit rapid assessment of risk vs. gain, and threat to intelligence capabilities vs. benefit to criminal prosecution. The number of variables is too high; the weights to be ascribed to those variables cannot be determined in advance; and the environment in which these decisions will have to be made cannot be foretold.

What is certain is that the intelligence world will continue to labor in the shadows, doing all it can to avoid Brandeis' sunlight, while the criminal justice system will do all it can to function under the noonday sun so that justice can "not only be done, but . . . manifestly and undoubtedly be seen to be done."[116]

115. *Aldrich Ames*, FED. BUREAU OF INVESTIGATION (2016), https://www.fbi.gov/history/famous-cases/aldrich-ames (last visited Oct. 2, 2017).

116. R. v. Sussex Justices, Ex parte McCarthy [1924] 1 KB 256, 259.