CHAPTER 8:

INDIVIDUAL REMEDIES, HOSTILE ACTORS, AND NATIONAL SECURITY CONSIDERATIONS

[1] This Chapter examines how individual remedies for privacy violations relate to the risk that hostile actors will use remedies to learn national security secrets. Part 2 of the Summary of Testimony discusses a central theme of my testimony, that we need systemic safeguards against excessive surveillance. Notably, systemic safeguards include transparency where feasible and oversight by institutions that have access to top secret information, such as the Foreign Intelligence Surveillance Court (FISC) and the Privacy and Civil Liberties Oversight Board (PCLOB). Part 3 of the Summary of Testimony examines the multiple ways that individuals can achieve remedies in the US for privacy violations. As discussed there, the US in numerous respects has a legal system that favors enforcement and individual remedies, including features such as: use of contingency fees (so a plaintiff does not need to be wealthy); parties pay their own litigation costs (so a losing plaintiff does not pay defendants' costs); jury trials; broad discovery rules; and easier certification of class actions.

[2] The Summary of Testimony also discusses a caveat about individual remedies in the intelligence setting. That caveat is the subject of the current Chapter. The desirability of individual remedies in intelligence systems must be weighed against the risks that come from disclosing classified information. In the terms used in Article 8 of the European Convention on Human Rights, the availability of the individual right to privacy for intelligence systems is assessed against the necessity in a democratic society of the interests of national security and public safety.

[3] The field of cybersecurity provides an analogy for deciding what types of remedies individuals should have about processing of their information by surveillance agencies. The idea I am suggesting is simple but I believe helpful – be cautious about creating a new vector of attack, such as individual remedies, into a protected system such as an intelligence agency.

[4] A simple example illustrates the sort of harm to national security that could result from individuals' direct access to their data held by an intelligence agency. Suppose a hostile actor, such as a foreign intelligence service, wants to probe the NSA or a Member State intelligence agency. The hostile actor may have Alice use a text service, Bob an email service, and Carlos a chat service. Each of them then file access requests, and only Bob has a file. If so, then the hostile actor has learned something valuable – the email service is under surveillance, but the text and chat services appear not to be. In this example, the individual remedy becomes an attack vector, or form of cyberattack – the hostile actor can probe the agency's secrets, and learn its sources and methods.

[5] Section I of this Chapter provides more detailed discussion of how a foreign intelligence agency or other hostile actor could use individual remedies to probe an intelligence agency, as a form of cyberattack. It also points out that attacks against intelligence agencies are not hypothetical – they occur every day by the most capable adversaries in the world. In short, restricted access to an intelligence agency's secrets can be seen predominantly as a security feature, rather than being a privacy bug.

[6] Sections II and III of this Chapter develop an important, related point – both European and US courts have already created doctrines to prevent this sort of attack. In the US, courts in certain instances recognize what is called the "state secrets doctrine," so that judges (while

maintaining overall supervision of a case) take care not to let individual litigation become a route of attack on national security secrets. Similar judicial decisions appear to be the norm in Europe, with judges protecting against disclosure or use of national security information in open proceedings. In other words, established law recognizes limits on individual remedies in the foreign intelligence area.

[7] Section IV of this Chapter discusses the importance of protecting individual rights in criminal cases, while also protecting classified secrets. I describe the US Classified Information Procedures Act (CIPA), which sets forth procedures for a criminal defendant to have access to classified information in a criminal case. Similar to my discussion of systemic safeguards, CIPA provides two important safeguards: (1) supervision by an independent judge; and (2) access by the judge and other participants to classified information, without disclosing classified information publicly.

I. Hostile Actors and the Analogy to Cybersecurity

[8] This Section briefly explains why intelligence agencies are high value targets for attack, including from the intelligence agencies and military operations of hostile actors. It explains the analogy to cybersecurity attacks, and concludes with a discussion of the risks of revealing national security secrets.

A. Intelligence Agencies are High Value Targets for Attack

[9] An intelligence agency such as the US National Security Agency or the German Bundesnachrichtendienst (BND) is a constant target for hostile actors, such as the military and intelligence services of adversary nations.[1] State secrets, including state surveillance secrets, are high value targets for hostile actors. Access by a hostile actor, for instance, could allow the hostile actor to gain access to: the surveillance information collected (including communications of data subjects); the types of services the agency is tracking; the specific targets under investigation; the identity of the agency's intelligence assets; and much more. Hostile actors may be especially interested in counterintelligence information – what does the agency under attack know about the hostile actor's own operations and possible spies within the agency? Suppose, at the extreme, that all of the NSA's and BND's activities were known to adversaries; in such a case, hostile terrorists or nation states would gain a large advantage against the NSA and BND, with in my view serious consequences to national security.

[1] Although any computer system today is subject to cyberattack, national intelligence agencies, with their numerous national security secrets, are subject to incessant attacks from advanced persistent threats. *Worldwide Cyber Threats: Hearing before the H. Permanent Select Comm. on Intelligence*, 114th Cong. 2 (Sept. 10, 2015) (statement of James R. Clapper, Dir. of National Intelligence) [hereinafter "*Worldwide Cyber Threats*"], https://fas.org/irp/congress/2015_hr/091015clapper.pdf ("Cyber threats to US national and economic security are increasing in frequency, scale, sophistication, and severity of impact."); Nicole Gaouette, *Intel chief: Presidential campaigns under cyber attack*, CNN.COM (May 18, 2016), http://www.cnn.com/2016/05/18/politics/presidential-campaigns-cyber-attack/ ("Clapper said in his decades-long career in intelligence, he doesn't 'recall a time when we've been beset by a wider array and more diverse array of threats and crises than we are today.'").

B. The Analogy to Cybersecurity Attacks

[10] As mentioned in the Introduction, the field of cybersecurity provides an analogy for deciding what types of remedies individuals should have about processing of their information by surveillance agencies. Many of us today are at least somewhat familiar with three types of cybersecurity precautions: (1) do not click on links in emails, because they might be phishing attacks; (2) update your antivirus software, so viruses will not infect your computer; and (3) have a good firewall, so attackers cannot get into your system. The idea I am suggesting is simple but I believe helpful – be cautious about creating a new vector of attack, such as individual remedies, into a protected system.

[11] One way to make the point is to ask the reader to imagine that you are the hostile actor. The thought experiment is to consider how the hostile actor could make use of the attack vector of individual remedies – what could the hostile actor learn, in what ways? The hostile actor could seek to gain information about the agency's sources and methods:

1. *Detect whether the agency is surveilling specific individuals.* The hostile actor can deploy Alice, Bob, Carlos, and others to send messages and make individual remedy requests. For the individuals whose messages were intercepted, the hostile actor learns specifically which individuals are under surveillance, and can draw inferences about what triggered those individuals' being under surveillance contrasted with those who were not.

2. *Detect surveillance selectors.* Alice could send a variety of messages with words or phrases she thinks might be selectors, and see which ones turn up in her individual remedy request. Information that Alice learns could be used to evade surveillance (avoid use of those selectors), or to feed strategic disinformation to the agency (use the selectors but tell the agency false information).

3. *Detect what channels are under surveillance.* As shown in the example, Alice might use a text service, Bob an email service, and Carlos a chat service. They then file access requests, and only Bob has a file. If so, then the hostile actor has learned something valuable – the email service is under surveillance, but the text and chat services appear not to be.[2]

4. *Unmask intelligence and counterintelligence agents.* During the Cold War, Soviet agents were discovered within Western intelligence agencies.[3] Alice could use her individual remedy to determine whether someone is assisting the agency's intelligence efforts. For instance, if Alice suspects an individual, Mallet, is sharing information with the agency, she could carefully feed that person sensitive information; if that information later turns up in Alice's file,

[2] Another possible inference is that Bob was under surveillance, but not Alice or Carlos. The hostile actor would thus have reason to conduct a series of probes, to test the hypotheses about the agency's sources and methods.
[3] JOHN EARL HAYNES AND HARVEY KLEHR, VENONA: DECODING SOVIET ESPIONAGE IN AMERICA (2000).

then she has gained evidence that Mallet is working with the agency. The hostile actor could then take action against Mallet, or could try to "turn" Mallet in order to feed incorrect information back to the agency.

[12] These examples illustrate how individual access requests by Alice and her colleagues could harm the intelligence agency's efforts to protect national security. Using the analogy to cybersecurity, the individual access request becomes a tool for probing the agency's defenses – access requests can "map" the agency's system the way that a hacker maps the computer systems under attack.

[13] Harms to the intelligence agency's activities can also occur if the individual remedy is indirect. Rather than allowing Alice to gain access to the intelligence agency's files, the access might be given to someone on Alice's behalf. For instance, the individual remedy might allow access by a data protection official, Danielle. This indirect approach would limit the number of persons with access to classified information held by the intelligence agency. This approach has the potential to provide an individual remedy for Alice, while reducing Alice's ability to gain inferences about the agency's source and methods.

[14] Providing access to the data protection official, Danielle, would nonetheless have certain risks:

1. *Moving classified information to an unclassified database has security risks.* To protect national security, classified information is only properly protected if: (a) the person accessing the information has a security clearance; and (b) the information is housed in a classified system. Moving classified information to an unclassified database thus is prohibited, and carries risk, unless there is an explicit and justified decision that the disclosure would no longer harm national security.

2. *The data protection official's system becomes a target for hostile actors.* If Danielle moves information about Alice to the data protection agency, then Danielle's system becomes a prime target for attack. Data protection agencies, and other non-military and non-intelligence systems, do not generally receive the resources to protect against determined attacks by nation-state actors.[4] This sort of cyberattack by nation states on non-intelligence actors became widely visible in 2016, with news reports about attacks against targets such as the Democratic National Committee and Hillary Clinton's campaign manager.[5] The possibility of a hack or breach is relevant to the overall

[4] European experts have expressed concerns about lack of adequate staffing and financial resources for data protection agencies, who sometimes "are not in a position to carry out the entirety of their tasks because of the limited economic and human resources available to them." European Union Agency for Fundamental Rights, *Data Protection in the European Union: the role of National Data Protection Authorities*, 42 (2010), http://fra.europa.eu/sites/default/files/fra_uploads/815-Data-protection_en.pdf; *Worldwide Cyber Threats*, *supra* note 1, at 3-4 (describing the risks and capabilities of state actors).

[5] *See* Nicole Gaouette, *Intel chief: Presidential campaigns under cyber attack*, *supra* note 1.

assessment of sending classified information into non-classified systems, such as to a data protection agency due to individual remedy requests.

3. *The data protection officials themselves become targets for hostile actors.* Again, considering the Cold War history of Soviet agents in Western intelligence agencies, there is the possibility that individuals such as Danielle could become targets for the hostile actors. Western intelligence agencies would face risks that a data protection official might reveal information due to sincere belief; for instance, individuals might believe they were principled whistleblowers, and decide to reveal classified information outside of lawful channels. There are also other ways that an official could be compromised, leading to disclosure of classified information.[6]

C. Risks of Revealing National Security Information

[15] In summary on the analogy to cyber-attacks, there are national security risks in creating a mechanism that reveals information held by the intelligence agency. Under US law, information is considered "top secret" if there would be "exceptionally grave damage" to national security if made publicly available.[7] Beyond "top secret," information held in US intelligence agencies is often "compartmentalized," with access only by individuals with a "Top Secret/Special Compartmentalized Information" security clearance. Intelligence information about named individuals is often, in my experience, available only to those with a TS/SCI clearance.[8]

[16] This extremely strict handling of personally identifiable information in the intelligence context is, in part, a privacy protection for the individual – there are strict limits on access to data about individuals who are not involved in the investigation of a crime, but whose information may arise during an intelligence investigation. The strict handling, in addition, is due to awareness of the risks to national security and the individual if the data becomes public. For instance, the information may be about someone cooperating with the US or an ally, but where the individual would be subject to harm if his identity was revealed. In terms used in Article 8 of

---

[6] I am not saying that there is any particular reason to believe that data protection officials would improperly disclose information. Instead, my point is that the history of intelligence agencies shows the possibility that the hostile actors will find ways to gain information unlawfully.

[7] *See* [2 PRINCIPLES FOR CLASSIFICATION OF INFORMATION] ARVIN S. QUIST, SECURITY CLASSIFICATION OF INFORMATION, *Ch. 7 Classification Levels* (1993) [hereinafter "SECURITY CLASSIFICATION OF INFORMATION"], https://fas.org/sgp/library/quist2/chap_7.html. In citing US law that states that an item marked "top secret" means that disclosure would cause "exceptionally grave challenge," I am not stating a view that every document marked "top secret" deserves "top secret" clearance. There is a considerable literature supporting the view that "over-classification" occurs in the US. *See, e.g.*, Dana Carver Boehm, *Guantanamo Bay and the Conflict of Ethical Lawyering*, 117 PENN ST. L. REV. 283 (2012); Alexandra Cumings & Kaplan v. Conyers, *Preventing the Grocery Store Clerk from Disclosing National Security Secrets*, 119 PENN ST. L. REV. 553 (2014); Jason B. Jones, *The Necessity of Federal Intelligence Sharing with Sub-Federal Agencies*, 16 Tex. Rev. L. & Pol. 175 (2011). My point, instead, is that there is national security risk in creating a system that permits outside individuals to probe the intelligence agency, revealing sensitive agency sources and methods.

[8] *See* SECURITY CLASSIFICATION OF INFORMATION, *supra* note 7, at *Appendix E Classification of Intelligence Information*.

the European Convention on Human Rights, such disclosures via an individual remedy could implicate the "rights and freedoms of others" if the data is revealed.

[17] In light of the strict control about access to intelligence information about a named individual, providing an individual remedy that gives outsiders access to that information raises national security risks. As discussed here, if the outside individual such as Alice can gain access to the information, then Alice and her colleagues can map the intelligence agency's activities. If a non-intelligence government employee can access the information, such as Danielle at the data protection agency, then Danielle would face a heightened risk of being subject to a nation-state level of attack. Consideration of the privacy advantages of such individual access should be weighed, in my view, with consideration of the national security risks as well.

II. The US State Secrets Doctrine

[18] Within the US, courts have established the state secrets doctrine to manage the usual rules for open judicial proceedings consistent with the risks to national security that can occur due to public disclosure. This section provides a brief overview of the doctrine. The purpose of the state secrets doctrine is to prevent litigation from disclosing sensitive material that could harm US national security. The doctrine requires the US government to state, through top level administration officials, that disclosure would threaten state secrets that would compromise national security. Courts examine the government's claim and independently determine – such as through *in camera* review of the material the government alleges to be harmful – whether disclosure in fact threatens American security interests. If the court agrees that a security threat exists, it excludes the material. The next Section of this Chapter describes similar doctrines in the EU.

A. Purpose of the State Secrets Doctrine

[19] The purpose of the state secrets doctrine is to protect national security, which would be endangered if information that could be used against the US were to be disclosed via judicial proceedings. A quote from the US Supreme Court illustrates the doctrine's national security focus:

> Many of the Government's efforts to protect our national security are well known. It publicly acknowledges the size of our military, the location of our military bases, and the names of our ambassadors to Moscow and Peking. But protecting our national security sometimes requires keeping information about our military, intelligence, and diplomatic efforts secret. We have recognized the sometimes-compelling necessity of governmental secrecy by acknowledging a Government privilege against court-ordered disclosure of state and military secrets.[9]

[9] *Gen. Dynamics Corp. v. United States*, 563 U.S. 478, 484 (2011) (internal citations omitted). US Supreme Court cases may be found at https://www.supremecourt.gov/opinions/opinions.aspx, or https://supreme.justia.com/. Appellate decisions offer insight into the gravity of harms the state secrets doctrine is used to prevent. Litigation can reveal sensitive military secrets, such as classified weapons systems. *See Zuckerbraun v. Gen. Dynamics Corp*., 935 F.2d 544, 547–48 (2d Cir. 1991), https://scholar.google.com/scholar_case?case=8505678271071925191&q=935+F.2d+544&hl=en&as_sdt=80006

Conversely, the state secrets doctrine "may not be used to shield any material not strictly necessary to prevent injury to national security."[10]

B. Procedure for Invoking the State Secrets Doctrine

[20] The procedure for invoking the state secrets doctrine shows the care that US courts take before providing an exception to the usual rule of open proceedings. The US Supreme Court states that the state secrets doctrine "belongs to the [g]overnment and must be asserted by it;" the doctrine "can neither be claimed nor waived by a private party."[11] To assert a state secrets claim, leaders of executive branch agencies must review information at issue in litigation, identify the national security threats litigation poses, and formally submit their concerns to the court under oath. Specifically, the "head of the department which has control over" the matter being litigated must personally lodge a "formal claim of privilege" with the court.[12] Moreover, the agency head may only make a formal state secrets claim after "actual personal consideration of the matter."[13]

[21] US courts require state secrets claims to be detailed. "Simply saying 'military secret,' 'national security' or 'terrorist threat' or invoking an ethereal fear that disclosure will threaten our nation is insufficient" to support state secrets claims; instead, "[s]ufficient detail" must be provided for courts to make a "meaningful examination."[14]

C. Independent Judicial Evaluation of Executive State Secrets Claims

[22] When a US agency head makes a formal state secrets claim, US courts examine the government's submissions and independently determine that litigation presents an actual threat to national security. In this evaluation, the emphasis is on the court's independence – the court must "assess the validity of the claim of privilege, satisfying itself that there is a reasonable danger that disclosure of the particular facts in litigation will jeopardize national security."[15]

[23] To evaluate governmental state secrecy claims, the court may inspect evidence the government claims would harm national security if disclosed, or it may rely on the declaration of

---

(case involving "weapons systems aboard the U.S.S. Stark"). It can damage the US's intelligence capabilities, *e.g.*, by disturbing relationships with intelligence assets, or by revealing the sources and methods intelligence agencies are using. *See CIA v. Sims*, 471 U.S. 159, 175 (1985) (noting that disclosure of methods "may compromise the Agency's ability to gather intelligence as much as disclosure of the identities of intelligence sources").

[10] *Ellsberg v. Mitchell*, 709 F.2d 51, 57 (D.C. Cir. 1983), https://scholar.google.com/scholar_case?case=14501985049476297 41&q=709+F.2d+51&hl=en&as_sdt=80006.

[11] *United States v. Reynolds*, 345 U.S. 1, 7 (1953).

[12] *Id.* In practice, heads of US agencies – *e.g.* the Director of National Intelligence or Attorney General – submit a declaration that (a) outlines his or her review of the matter, (b) states his or her personal knowledge, and (c) explains with particularity the harms to national security he sees resulting from the disclosure of sensitive materials.

[13] *Id.* at 7-8. For a case rejecting the government's attempt to assert the state secrets doctrine because the agency director claiming the privilege did not "personally conside[r] the material for which the privilege is sought," *see Yang v. Reno*, 157 F.R.D. 625, 634 (M.D. Pa. 1994).

[14] *Al-Haramain Islamic Found., Inc. v. Bush*, 507 F.3d 1190, 1203 (9th Cir. 2007), https://scholar.google.com/scholar_case?case=5006140604567331133&q=507+F.3d+1190&hl=en&as_sdt=80006.

[15] *Zuckerbraun*, 935 F.2d at 546.

the agency director.[16] Generally speaking, if evidence is essential to a party's case, an *in camera* inspection is conducted; if the government raises plausible and substantial allegations of danger, a court may rely on the government's declaration.[17]

[24] Case law requires US courts to scrutinize government state secrets claims in the interest of upholding democratic commitments to open judicial proceedings. The Supreme Court has stated that the doctrine is "not to be lightly invoked."[18] Courts must "critically [] examine instances of [the state secrets doctrine's] invocation" in order to "ensure that [it] is asserted no more frequently and sweepingly than necessary."[19] State secret decisions place courts under the "special burden" of ensuring "that an appropriate balance is struck between protecting national security matters and preserving an open court system."[20]

[25] Cases reflect US courts carefully examining attempts to invoke the state secrets privilege:[21] "We take very seriously our obligation to review [government state secrets claims] with a very careful, indeed a skeptical, eye, and not to accept at face value the government's claim or justification of privilege."[22] Moreover, the court "must scrutinize the claim of privilege more carefully when the plaintiff has 'made a compelling showing of need for the information in question.'"[23]

D. Further Proceedings after Successful State Secrets Claims

[26] If judges independently determine that litigation threatens to harm national security, US cases hold they must prevent that harm from occurring. Evidence posing a national security risk must be "completely removed from the case."[24] Thus, when courts determine that state secrets must be kept out of proceedings, they must also determine "how the matter should proceed in light of the successful privilege claim."[25] In many cases, proceedings will go forward without

---

[16] The court's procedure is guided by the principle of not "forcing a disclosure of the very thing the [state secrets] privilege is designed to protect." *See Reynolds*, 345 U.S. at 8.
[17] *See Ellsberg*, 709 F.2d at 58–59 ("[T]he more compelling a litigant's showing of need for the information in question, the deeper the court should probe in satisfying itself that the occasion for invoking the privilege is appropriate.") (internal citations and quotation marks omitted).
[18] *Reynolds*, 345 U.S. at 7.
[19] *Ellsberg*, 709 F.2d at 58.
[20] *Al-Haramain*, 507 F.3d 1203.
[21] For example: "We have spent considerable time examining the government's declarations (both publicly filed and those filed under seal). We are satisfied that the basis for the privilege is exceptionally well documented. Detailed statements underscore that disclosure of information concerning the Sealed Document and the means, sources and methods of intelligence gathering in the context of this case would undermine the government's intelligence capabilities and compromise national security. Thus, we reach the same conclusion as the district court: the government has sustained its burden as to the state secrets privilege." *Id.* at 1203-04.
[22] *Id.* at 1203.
[23] *In re Sealed Case*, 494 F.3d 139, 144 (D.C. Cir. 2007) (quoting *Ellsberg*, 709 F.2d at 59 n. 37, 61), https://scholar.google.com/scholar_case?case=15677361886209895 08&q=494+F.3d+139&hl=en&as_sdt=80006.
[24] *Kasza v. Browner*, 133 F.3d 1159, 1166 (9th Cir. 1998), https://scholar.google.com/scholar_case?case=4720850483028952155&q=133+F.3d+1159&hl=en&as_sdt=80006.
[25] *Al-Haramain*, 507 F.3d at 1202 (internal citation omitted).

the excluded evidence,[26] and can proceed to discovery and trial as long as plaintiffs can prove the "essential facts" of their claims "without resort to material touching upon military secrets."[27] In some cases, however, a successful state secrets claim can lead to dismissal of the proceedings or of certain claims.[28]

III. Similar State Secrets and Public Interest Doctrines in EU Member States

[27] Similar to the US state secrets doctrine, EU Member States have established doctrines to prevent national security information from being disclosed in litigation. I present summaries of my research, alphabetically, for: (A) French statutes criminalizing use of classified information in court proceedings; (B) the German governmental secrecy objection; (C) Irish privilege doctrines relevant to the security of the state; (D) the Italian state secrets privilege; and (E) the United Kingdom's doctrine of public interest immunity.

[28] The similarity of these US and EU doctrines, in my view, puts into perspective the earlier discussion of the risks of hostile actors using individual remedies to learn the secrets of US and EU intelligence agencies. The discussion about the cybersecurity style attacks by hostile actors illustrated national security risks from granting access by individuals to intelligence agency information. The discussion about US and EU state secret doctrines show a basic similarity of how courts are aware of the risk of revealing national security secrets, and limit the ability of litigants to use individual remedies to compromise national security.

A. France: Criminal Sanctions for Disclosing State Secrets in Court

[29] French statutes create criminal penalties for accessing or disclosing classified information in judicial proceedings. Under France's Defense Code, individual executive agencies (such as

---

[26] "The effect of the government's successful invocation of the state secrets privilege . . . is well established: '[T]he result is simply that the evidence is unavailable, as though a witness had died, and the case will proceed accordingly, with no consequences save those resulting from the loss of the evidence.'" *Ellsberg*, 709 F.2d at 64 (quoting 2 McCormick on Evidence § 233 (E. Cleary ed. 1972)).

[27] *Al-Haramain*, 507 F.3d at 1204 (quoting *Reynolds*, 345 U.S. at 11).

[28] Decisions recognize that in rare cases, "the very subject matter of the action" is a state secret, *see Reynolds*, 345 U.S. at 11 n.26 (citing *Totten v. United States*, 92 U.S. 105 (1875)), or that state secrets are "so central to the subject matter of the litigation that any attempt to proceed will threaten disclosure of the privileged matters," *Fitzgerald v. Penthouse Int'l, Ltd*., 776 F.2d 1236, 1241-42 (4th Cir. 1985), https://scholar.google.com/scholar_case?case=3765361197667528388q=776+F.2d+1236&hl=en&as_sdt=80006. In such cases, the court has discretion to dismiss proceedings in full or in part. Courts have done so, for example, when individual litigation would require the government to identify the location of nuclear weapons. *See Weinberger v. Catholic Action of Hawaii/Peace Educ. Project*, 454 U.S. 139 (1981). Also, a case challenging a program under Section 702 of FISA has been dismissed because the court determined it would "risk informing adversaries of the specific nature and operational details" of the program. *Jewel v. Nat'l Sec. Agency*, No. C 07-00693 JSW, 2015 WL 545925, at *5 (N.D. Cal. Feb. 10, 2015), http://www.leagle.com/decision/In%20FDCO%2020150211A45/Jewel%20v.%20National%20Security%20Agency. In these rare cases, US courts describe dismissal as "ultimately the less harsh remedy" because it vindicates "the greater public good" of protecting the nation and its citizens. *Bareford v. Gen. Dynamics Corp*., 973 F.2d 1138, 1144 (5th Cir. 1992), https://scholar.google.com/scholar_case?case=7680050268108144567&q=973+F.2d+1138&hl=en&as_sdt=80006, opinion vacated in part on denial of reargument (Oct. 14, 1992).

the Ministry of Defense) are responsible for classifying information.[29] Article 413-9 of France's Penal Code declares classified information to constitute national defense secrets.[30] Accessing, learning the content of, reproducing, or making defense secrets public is a crime punishable by five years' imprisonment or a fine of € 75,000.[31]

[30] Judges may not access or use defense secrets in judicial proceedings, nor may parties disclose them, unless the secrets are first declassified – otherwise, the judge or disclosing party commits a crime under Article 413 of France's Penal Code.[32] Instead, France's Law No. 98-567 creates a Consultative Commission on National Defense Secrets (CCNDS).[33] When a court encounters classified materials and wishes to declassify them for use in judicial proceedings, it can petition the CCNDS for a classification review.[34] The CCNDS will issue a recommendation as to whether the documents at issue should remain secret. However, the ministry or agency that originally classified the information is not bound by the CCNDS's declassification recommendation.[35] It may continue to refuse to declassify materials.[36] As a result, unless executive agencies agree to declassify materials sought to be used in court, French law effectively excludes the materials from use in judicial proceedings.[37]

---

[29] *See* CODE DE LA DÉFENSE [DEFENSE CODE], particularly at Arts. R.*1132 *et seq.* (Fr.), (in French) https://www.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT000006071307.

[30] *See* CODE PÉNAL [PENAL CODE], Art. 413-9, (in French) https://www.legifrance.gouv.fr/affichCodeArticle.do?cidTexte=LEGITEXT000006070719&idArticle=LEGIARTI000006418400.

[31] *Id.* at Art. 413-11.

[32] *See id.* at Arts. 413-9-413-11.

[33] *See* Loi 98-567 du 8 juillet 1998 instituant une Commission consultative du secret de la défense nationale [Law of 8 July 1998 Instituting a Consultative Commission on National Defense Secrets], JOURNAL OFFICIEL DE LA RÉPUBLIQUE FRANÇAISE [OFFICIAL GAZETTE OF FRANCE] July 9, 1998, p. 10488, Art. 1 [hereinafter "CCNDS Law"], (in French) https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000389843&categorieLien=id.

[34] *Id.* Art. 4.

[35] *See* MINISTÈRE DE LA DÉFENSE [DEFENSE MINISTRY], SECRÉTARIAT GÉNÉRAL POUR L'ADMINISTRATION [SECRETARY-GENERAL FOR ADMINISTRATION], *Secret Défense* [Defense Secrets] (Sept. 17, 2012), (in French) http://www.defense.gouv.fr/sga/le-sga-en-action/droit-et-defense/secret-defense/secret-defense (noting that the CCSND's declassification recommendations are not binding on ministries).

[36] The CCNDS's recommendations are published in France's Official Journal independent of whether the ministry elects to follow them. *See* CCNDS Law, *supra* note 33, Art. 8.

[37] France's Constitutional Council has held that the prohibition on judges accessing classified materials is unconstitutional as applied to a magistrate who, in the course of exercising his duty to investigate facts, accesses a classified physical area. *See* Conseil Constitutionnel [CC] [Constitutional Council], decision No. 2011-192 QPC, Nov. 10, 2011, at para. 37 ("*Ekaterina*"), (in English) http://www.conseil-constitutionnel.fr/conseil-constitutionnel/english/case-law/decision/decision-no-2011-192-qpc-of-10-november-2011.104102.html. The Council, however, deemed the remainder of the classification regime described above to be constitutional. *See id.* at para. 28 *et seq.*

B. Germany: the Governmental Secrecy Objection

[31] Germany has codified a governmental secrecy doctrine in Section 99 of the Code of Administrative Court Procedure (CACP) (*Verwaltungsgerichtsordnung*).[38] This provision permits government agencies to refuse to produce any documents or information that (a) "would prove disadvantageous to the interests of the Federation or of a [State]," or that (b) "must be kept strictly secret in accordance with a statute" or "due to their essence."[39] German court decisions require courts to examine *in camera* materials over which government entities claim secrecy.[40] In response, the German legislature enacted *in camera* review procedures that show concern for litigation against the government becoming an avenue for revealing state secrets:

- Once a government agency has raised national security objections to production, the party seeking the documents or information may lodge a motion for *in camera* review.

- The trial court does not conduct the *in camera* review. Instead, if a top level federal agency (such as the Ministry of Defence) contends that disclosing information would harm Germany's national security, Germany's Supreme Administrative Court (SAC) – the court of last resort in the administrative court system – conducts the *in camera* review via an interlocutory proceeding.[41]

- The SAC has created a Special Panel (*Fachsenat*) to conduct *in camera* reviews of sensitive evidence.[42] The Special Panel's rulings are final, and no appeal is permitted.[43]

---

[38] In Germany, suits against the government or a federal or state agency must generally be filed in the administrative courts. Accordingly, the CACP contains the rules by which government agencies can keep sensitive information out of public court proceedings.

[39] VERWALTUNGSGERICHTSORDNUNG, [VWGO] [CODE OF ADMINISTRATIVE COURT PROCEDURE] § 99(1) [hereinafter "CACP"], (in English) https://www.gesetze-im-internet.de/englisch_vwgo/englisch_vwgo.html.

[40] Until the 1990s, courts were permitted to rely on agency assertions that evidence was potentially harmful and should not be disclosed. In 1999, the German Constitutional Court required that administrative courts conduct *in camera* review of the material. *See* BVerfG [Federal Constitutional Court], decision of the First Senate of 27 October 1999, 1 BvR 385/90, (in German) https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/1999/10/rs19991027_1bvr038590.html.

[41] Both the German government as well as its administrative court system are arranged along federal lines. If a state agency, or a lower-level federal agency, invokes a secrecy claim, the interlocutory *in camera* review is first conducted by a special panel of the Administrative Court of Appeal (*Oberverwaltungsgericht*) in the German state where proceedings are pending; its decision can be appealed to the SAC's Special Panel. If a top-level federal agency – such as the Ministry of Defence, Interior Ministry, etc. – invokes public interests (such as national security) against production, the interlocutory *in camera* review goes directly to the SAC. The secrecy requirements outlined in this section apply to both types of *in camera* proceedings. *See* CACP, *supra* note 39, at § 99(2).

[42] For a decision of the SAC Special Panel, *see, e.g.*, BVerwG [Supreme Administrative Court], judgment of 26 August 2004, BVERWG 20 F 19.03, (in German) http://www.bverwg.de/entscheidungen/entscheidung.php?ent=260804B20F19.03.0. In this decision, the Special Panel notes that the German legislature designed the *in camera* proceedings of CACP § 99 to minimize the number of persons who gain access to potentially sensitive materials. For the same reason, the court states that each German administrative appellate court obligated to conduct Section 99 *in camera* reviews created "only one" special panel. *Id.* at para. 7.

- Proceedings before the SAC's Special Panel are conducted in secret,[44] and all judges and court personnel are bound to maintain secrecy.[45] If the agency asserting privilege states that "special reasons of confidentiality or classification" are present, it can require review to be conducted within the agency's own offices.[46]

- The SAC's order resolving the privilege claim "may not provide an indication of the nature and content of the secret certificates, files, documents and information."[47]

[32] If the SAC determines that documents present a danger to German security that outweighs the interest in disclosure, the documents are barred from being used in the underlying court proceedings. In addition to documentary evidence, German agencies can prohibit individuals from testifying on sensitive matters – and if the SAC finds that testimony would harm national security, it can prohibit plaintiffs from testifying on their own behalf to the extent it would touch on sensitive matters.[48] If evidence or testimony is essential to a claim, SAC exclusion decisions can lead to a dismissal or other form of adverse judgment.

C. Irish Privilege Doctrines relevant to the Security of the State

[33] In Ireland, courts apply doctrines of public interest privilege and statutory privilege in situations where "the vital interests of the State (such as the security of the State)" may be harmed through information disclosed in judicial proceedings.[49] Public interest privilege is a claim that – with regard to documents at issue in litigation – the public's general interest in open proceedings is outweighed by another public interest of higher order, such as State security.[50] Statutory privilege is an assertion that a statute prohibits disclosure, such that a statutorily recognized public interest justifies keeping certain documents or information confidential.[51]

---

[43] CACP, *supra* note 39, at § 99(2).
[44] *Id.*, 7th sentence.
[45] *Id.*, 10th sentence.
[46] *Id.*, 8th sentence.
[47] *Id.*, 10th sentence.
[48] For an example of the Special Panel upholding an agency-imposed prohibition on testifying on sensitive matters, *see* BVerwG [Supreme Administrative Court], Judgment of 26 August 2004, BVERWG 20 F 19.03, (in German) http://www.bverwg.de/entscheidungen/entscheidung.php?ent=260804B20F19.03.0.
[49] *See Murphy v. Corporation of Dublin* [1972] IR 215, 283 (S.C.) ["*Murphy*"].
[50] *See, e.g., Livingstone v. Minister for Justice* [2004] IEHC 58 at § 6 (H. Ct.), http://www.bailii.org/ie/cases/IEHC/2004/58.html, (describing public interest privilege as a balancing of "the public interest in the proper administration of justice by making all relevant material available to litigants, and the public interest in not harming society as a whole by releasing highly confidential State information in respect of which public interest immunity is claimed").
[51] Statutory privilege appears to have been first recognized in *Cully v. Northern Bank Finance Corp.* [1984] ILRM 683, and more recently applied in *O'Brien v. Ireland* [1995] 1 IR 568 (H.C.).

[34] Public interest or statutory privilege claims must be asserted by "the person seeking the privilege;"[52] in the context of litigation posing risks to State security, government ministers and An Garda Síochána officers of appropriate rank have asserted such privilege claims.[53] Like in the US, Irish courts "closely scrutinise"[54] the claim and independently determine whether the general interest in open proceedings is in fact outweighed by a weightier public interest, such as State security.[55] In making this determination, courts may examine the documents over which privilege has been claimed. At the same time, "[t]here is no obligation on the judicial power to examine any particular document," and courts "can and will in many instances uphold a claim of privilege in respect of a document merely on the basis of a description of its nature and contents."[56]

[35] Irish courts have applied public interest and statutory privileges to prevent sensitive information from being disclosed in cases implicating significant security interests. The Supreme Court's decision in *Murphy v. Corporation of Dublin* states that courts should intervene in litigation to preserve national security,[57] and permit even the existence of documents to be withheld when serious harm is threatened.[58] Further cases have stated that in general, litigation should not disclose confidential information about An Garda Síochána's sources,[59] methods,[60] or ongoing investigations.[61] In *Keating v. Radio Telefís Éireann*, the High Court refused to permit inspection or discovery of documents relating to An Garda's witness protection program, finding that doing so would harm "the prevention and detection and prosecution of crime" and would "put at risk the lives and wellbeing of the individuals" involved in the program.[62] Additionally, in *O'Brien v. Ireland*, the High Court refused to permit an Irish soldier's widow from discovering court of inquiry reports about his death during a UN peacekeeping mission, after the

---

[52] *McLoughlin v. Aviva Insurance (Europe) Public Ltd. Co.* [2011] IESC 42 (Transcript), http://www.bailii.org/ie/cases/IESC/2011/S42.html.

[53] *See, e.g.*, *Keating v. Radio Telefís Éireann* [2013] IEHC 393, http://courts.ie/Judgments.nsf/0/8CF48D7FA15CB2A080257BD4004CF393, for an example of affidavits claiming public interest privilege submitted by Garda officers.

[54] *Id.*

[55] *Ambiorix Ltd. v. Minister for the Environment* [1992] 1 I.R. 277, 283 (S.C.) ("Where a conflict arises during the exercise of the judicial power between the aspect of public interest involved in the production of evidence and the aspect of public interest involved in the confidentiality or exemption from production of documents . . . , it is the judicial power which will decide which public interest shall prevail.").

[56] *Id.* at 284.

[57] *Murphy* [1972] I.R. at 283-284 ("It is clear that, when the vital interests of the State (such as the security of the State) may be adversely affected by disclosure or production of a document, greater harm may be caused by ordering rather than by refusing disclosure or production of the document.").

[58] *Id.* ("[I]n certain circumstances the very disclosure of the existence of a document, apart altogether from the question of its production, could in itself be a danger to the security of the State.").

[59] *See Skeffington v. Rooney* [1997] 1 IR 22 (S.C.) (the "countervailing public interest [] in the detection and prevention of crime [] has led the courts . . . to allow the anonymity of police informers to be preserved").

[60] *See Breathnach v. Ireland* [1993] 2 IR 458 (H.C.) ("[T]here may be material the disclosure of which would be of assistance to criminals by revealing methods of detection or combatting crime," which is "a consideration of particular importance today when criminal activity tends to be highly organised and professional.").

[61] *See McLoughlin* [2011] IESC 42 at para. 12 (Transcript) ("[I]n general documents material to an ongoing criminal investigation by An Garda Síochána should not be required to be disclosed in civil proceedings.").

[62] *Keating* [2013] IEHC 393.

government asserted that permitting discovery "may endanger not only the Irish battalion, but the United Nations peace-keeping force generally."[63]

[36] In addition to case law, provisions in Ireland's Criminal Justice (Surveillance) Act, 2009 (CJA)[64] show hesitancy to disclose information about Irish surveillance in judicial proceedings. Under Section 15 of the CJA, "the existence or non-existence" of surveillance or facts related to it "shall not be disclosed by way of discovery or otherwise in the course of any proceedings."[65] Courts "shall not authorize" disclosure of such information if doing so is likely to create a material risk to (a) "the security of the State;" (b) counterterrorism activities; or (c) the "integrity, effectiveness and security" of Garda or Irish Defence Forces operations.[66] Courts may only authorize disclosure of surveillance-related information if "in all of the circumstances it is in the interests of justice to do so," and "subject to such conditions as [the court] considers justified."[67]

D. Italy: the State Secrets Privilege

[37] Within Italy, statutory rules and court decisions ensure that matters designated as state secrets will not be disclosed through judicial proceedings. Italian statutes prohibit "public officials, public employees and public service providers" from disclosing information that has been classified as a state secret in court proceedings.[68] When a state secrecy objection is raised, the court must determine whether the evidence at issue is essential to the proceedings. If it is, the court must (a) stay any proceedings that could disclose secret matters, and (b) request the Italian Prime Minister to confirm "the existence of State secret status" over the materials at issue.[69] The Prime Minister has 30 days to respond via a reasoned explanation.[70]

[38] If the Prime Minister confirms state secrets are in fact threatened with disclosure, the trial court may elect to exclude the secret material and, depending on its importance, dismiss the proceedings.[71] Alternatively, the court may challenge the Prime Minister's secrecy classification by ordering an interlocutory appeal to Italy's Constitutional Court.[72] The Constitutional Court,

---

[63] *O'Brien v. Ireland* [1995] 1 IR 568 (H.C.). The Court held the court of inquiry reports were covered by statutory privilege. *See id.* (citing the Diplomatic Relations and Immunities Act, 1967; the Defence Act, 1954; and the Defence Forces Rules of Procedure, 1954).

[64] *See* Criminal Justice (Surveillance) Act 2009 (Act. No. 19/2009) (Ir.), http://www.irishstatutebook.ie/eli/2009/act/19/section/15/enacted/en/html#sec15.

[65] *Id.* § 15(1).

[66] *Id.* § 15(2).

[67] *Id.* § 15(3).

[68] Legge 124/2007: Sistema di informazione per la sicurezza della Repubblica e nuova disciplina del segreto [Law no. 124/2007: System of Intelligence for the Security of the Republic and New Provisions on Secrecy] § 41(1) (It.) [hereinafter "Italian Intelligence & Secrecy Law"], (in English) https://www.sicurezzanazionale.gov.it/sisr.nsf/english/law-no-124-2007.html. "State secrets" are defined as information whose disclosure "may be used to damage the integrity of the Republic (including in relation to international agreements, the defence of its underlying institutions as established by the Constitution, the State's independence vis à vis other states and its relations with them, as well as its military preparation and defence)." *Id.* § 39(1). The Prime Minister is responsible for classifying matters as state secrets. *See id.* § 39(5).

[69] *Id.* § 41(2).

[70] *Id.* § 41(4), (5).

[71] *Id.* § 41(3).

[72] *Id.* § 41(8).

however, has stated it will not review the Prime Minister's secrecy classification on the merits, *i.e*. it will not decide whether the information is properly classified. The Constitutional Court has interpreted its duty narrowly, as limited to confirming that the Prime Minister has followed the statutory procedure for claiming secrecy over the materials at issue.[73] The court explains its refusal to examine secrecy claims as follows: "the choice of the necessary and appropriate means to ensure national security is a political one, belonging, as such, to the Executive branch and not to the ordinary judiciary."[74] As a result, the executive's assertion of state secrecy will likely bind the Italian courts.

[39] A successful state secrecy objection prohibits the Italian court "from acquiring or using the information having State secret status even indirectly."[75] Although the court is not prohibited from proceeding on the basis of "elements existing separately and independently of the records, documents or matters having State secret status,"[76] if secret evidence is essential to the claims, "the judge shall state that he/she cannot proceed on account of the existence of a State secret."[77]

E. United Kingdom: the Public Interest Immunity Doctrine

[40] In the United Kingdom, courts apply the doctrine of public interest immunity (PII) as a response to litigation that threatens to disclose information that could harm national security. PII is a claim that given the sensitive nature of particular documents, "it would be injurious to the public interest" to disclose them or produce them for inspection.[78] If a PII claim is successfully asserted, evidence is excluded from litigation.

[41] Similar to the US approach, PII claims must be asserted by the UK government. To assert a PII claim, the minister with responsibility for the information in question submits a certificate to the court detailing why disclosure or production would harm the UK's interests.[79] UK courts then independently determine whether, with regard to the documents at issue, higher order public interests (such as national security) outweigh the interest in open judicial proceedings. To make this determination, UK courts may inspect the documents over which the government has claimed privilege.[80]

---

[73] *See* Corte Constituzionale [Constitutional Court], 11 marzo 2009, Judgment 106/2009 ("*Abu Omar*") (adopting limited review of the Prime Minister's secrecy assertions), (in Italian) http://www.cortecostituzionale.it/actionSchedaPronuncia.do?anno=2009&numero=106; Corte Constituzionale [Constitutional Court] 29 febbraio 2012, Judgment 40/2012 ("*Abu Omar*") (affirming 2009 ruling), (in Italian) http://www.cortecostituzionale.it/actionSchedaPronuncia.do?anno=2012&numero=40; Corte Constituzionale [Constitutional Court] 19 febbraio 2014, Judgment 24/2014 ("*Abu Omar*") (reaffirming 2009 ruling), (in Italian) http://www.cortecostituzionale.it/actionSchedaPronuncia.do?anno=2014&numero=24.

[74] *See* Corte Constituzionale [Constitutional Court], 11 marzo 2009, Judgment 106/2009 ("*Abu Omar*"), at para. 3, (in Italian) http://www.cortecostituzionale.it/actionSchedaPronuncia.do?anno=2009&numero=106.

[75] Italian Intelligence & Secrecy Law, *supra* note 68, at § 41(5).

[76] *Id.* § 41(6).

[77] *Id.* § 41(3).

[78] *Duncan v. Cammel Laird & Co. Ltd.* [1942] AC 624, 627 (H.L.) (UK), http://www.bailii.org/uk/cases/UKHL/1942/3.html.

[79] *Id.* at 638.

[80] *Conway v Rimmer* [1968] AC 910 (H.L.) (UK), http://www.bailii.org/uk/cases/UKHL/1968/2.html.

[42] In cases where litigation threatens national security, UK courts have held that they should afford deference to the executive's claim of privilege and may need to avoid *in camera* inspections, because evaluating the national security implications of documents goes beyond the judiciary's traditional expertise.[81] Thus, in national security cases, evidence should be excluded as long as the minister's certificate substantiates an actual or potential risk to UK security.[82]

[43] As an alternative to asserting a PII claim, UK law has recently provided the option of requesting the court to hold a Closed Material Proceeding (CMP).[83] In a CMP, evidence that would otherwise be excluded via a PII claim is instead evaluated by the court in a secure, "closed" proceeding.[84] Special Advocates are appointed to represent the interests of non-governmental parties.[85] The court then issues a ruling or judgment that adjudicates the parties' rights, but does not disclose classified information.[86] The purpose of a CMP is to provide a judicial determination based on evidence – as opposed to a dismissal due to a PII claim – while making sure that information that could be used to harm UK interests is not disclosed.

---

[81] *See, e.g., Balfour v. Foreign and Commonwealth Office* [1993] ICR 663 (E.A.T.) (UK), http://www.bailii.org/uk/cases/UKEAT/1993/182_92_1210.html: "[There are] two separate categories of situations where the public interest is involved. The first [is] where the reasons given are susceptible of being weighed by judicial experience, and there the judge has to do the weighing or balancing process which usually involves an inspection by him[;] and the second [is] where the reasons given by the Minister are of a character which judicial experience is not competent to weigh. In the latter case, the judge by definition has no effective means for weighing the reasons adduced but it is still his function to perform the balancing act between the two public interests, one of the proper administration of justice which requires relevant evidence to be disclosed and not hidden, the other the protection of national security. [I]t will be the latter that will prevail, if . . . evidence of the necessary factual link between the documents and the reasons adduced is produced."

[82] *See Balfour v. Foreign and Commonwealth Office* [1994] 2 All ER 588, [1994] 1 W.L.R. 681, 688 (C.A.) (UK) ("There must always be vigilance by the courts to ensure that public interest immunity of whatever kind is raised only in appropriate circumstances and with appropriate particularity, but once there is an actual or potential risk to national security demonstrated by an appropriate certificate the court should not exercise its right to inspect.")

[83] *See* Justice and Security Act 2013 c. 18 (UK) [hereinafter "JSA"], http://www.legislation.gov.uk/ukpga/2013/18/pdfs/ukpga_20130018_en.pdf. Under the JSA, CMPs are available for civil, immigration, and employment proceedings.

[84] The court may invoke CMPs whenever it finds that (a) a party would be required to disclose "material the disclosure of which would be damaging to the interests of national security" during proceedings; and (b) the interests of justice favor proceeding via CMP. *See* JSA §§ 6(4), (5), (11).

[85] *See* JSA § 9. To protect secrecy, parties represented by a Special Advocate do not know who the advocate is, nor is the advocate "responsible to the party to the proceedings whose interests the person is appointed to represent." JSA § 9(4).

[86] Depending on the kind of rights the court is adjudicating, European Court of Human Rights decisions that have been adopted by the English courts may require it to provide the 'gist' of its reasoning to an affected individual.

IV. US Criminal Proceedings under the Classified Information Procedures Act

[44] The US Classified Information Procedures Act (CIPA) protects criminal defendants' rights while preventing disclosure of classified national security information.[87] As with the US systemic safeguards for foreign intelligence investigations, CIPA provides two important protections: (1) supervision by an independent judge; and (2) access by the judge and other participants to classified information, without disclosing classified information publicly.

[45] CIPA is designed to "protec[t] and restric[t] the discovery of classified information in a way that does not impair the defendant's right to a fair trial."[88] CIPA governs criminal proceedings where classified information may be disclosed.[89] CIPA is not designed to change defendants' substantive rights; instead, it is a "procedural framework for ruling on questions of admissibility involving classified information before introduction of the evidence in open court."[90]

[46] This section outlines criminal proceedings under CIPA. CIPA applies when the court enters a protective order governing how parties are to handle classified information during proceedings. The government must then satisfy constitutional and statutory discovery obligations, potentially – subject to court approval – producing substitutes for some items of classified evidence. After discovery, the defense must give notice of the classified information it anticipates using at trial. This results in a hearing at which the court determines which classified items are admissible as evidence. The government can then ask the court for permission to use substitutes of classified items the court has deemed admissible. If the court refuses, the government must either permit disclosure or suffer an adverse order.

A. Protective Order

[47] CIPA applies when the government asks the court to enter a protective order for classified information. Pursuant to CIPA, the US Judicial Branch has adopted security procedures for protecting classified information in federal courts.[91] The court enters a protective

---

[87] CIPA is codified at 18 U.S.C. App. III §§ 1-16, and is available in its entirety at https://www.law.cornell.edu/uscode/html/uscode18a/usc_sup_05_18_10_sq3.html.

[88] *United States v. O'Hara*, 301 F.3d 563, 568 (7th Cir. 2002), https://scholar.google.com/scholar_case?case=2763159407792597911&q=301+F.3d+563&hl=en&as_sdt=80006. CIPA also attempted to alleviate "the growing problem of greymail," *i.e*. "a practice whereby a criminal defendant threatens to reveal classified information during the course of his trial in the hope of forcing the government to drop the criminal charge against him." *United States v. Anderson*, 872 F.2d 1508, 1514 (11th Cir. 1989), https://scholar.google.com/scholar_case?case=12402375278722086310&q=872+F.2d+1508&hl=en&as_sdt=80006.

[89] Classified information is defined as "any information or material that has been determined by the United States Government pursuant to an Executive order, statute, or regulation, to require protection against unauthorized disclosure for reasons of national security." CIPA § 1(a), codified at 18 U.S.C. App. III § 1(a).

[90] *Anderson*, 872 F.2d at 1514.

[91] Section 9 of CIPA required the Chief Justice of the US Supreme Court to "prescribe rules establishing procedures for the protection against unauthorized disclosure of any classified information in the custody of the United States." CIPA § 9(a), codified at 18 U.S.C. App. III § 9(a). The security procedures currently in force are codified at 18 U.S.C. App. III § 9 note (issued Feb. 12, 1981) [hereinafter "Judicial Branch Security Procedures"].

order consistent with these procedures, to govern how classified information is handled during the case.[92]

[48] The Judicial Branch's security procedures generally require defense attorneys to obtain a security clearance in order to receive and view classified information.[93] The court gives defense attorneys an opportunity to apply for security clearances if they do not yet have one. The court also appoints a member of the US Department of Justice's Management Division as a Court Security Officer (CSO),[94] to assist defense attorneys in obtaining appropriate clearances. Upon receiving security clearances, defense lawyers can review the relevant classified information.[95]

B. Discovery

[49] After entry of a protective order, CIPA cases move to the discovery phase. As with other US criminal proceedings, the prosecution is subject to discovery obligations, such as producing exculpatory evidence (evidence that tends to weaken the prosecution's case).[96] CIPA does not change the scope of these discovery obligations,[97] but introduces a court-mediated procedure for production. The court inspects the submitted evidence *in camera* and determines what evidence is discoverable.[98]

[50] Classified items the court deems discoverable are produced to the defense. The government, however, may argue that national security would be harmed if particular items were produced, and propose substitutes for those items.[99] The court then determines whether the government has made a "sufficient showing,"[100] and may approve substitutes of classified evidence to be produced.[101] CIPA permits substitutes such as: (a) summaries of information from classified documents; (b) admissions of facts classified evidence would prove; or

---

[92] *See id.* § 3. The government must request the protective order by filing a motion that sets forth the national security concerns the case raises. If the government requests a protective order, CIPA requires the court to issue it. *See id.*

[93] *See* Judicial Branch Security Procedures, *supra* note 91.

[94] *See id.* § 2 ("In any proceeding in a criminal case . . . in which classified information is within, or reasonably expected to be within, the custody of the court, the court shall designate a court security officer.").

[95] If defense attorneys are unable to obtain a security clearance, they may seek an exemption order from the court. Alternatively, the court can permit a security cleared co-counsel to assist the defense.

[96] Exculpatory evidence is referred to as "*Brady* material" after the US Supreme Court case that required its production. *See Brady v. Maryland*, 373 U.S. 83 (1963). The Federal Rules of Criminal Procedure set forth additional categories of evidence the government must produce, including: (a) any item obtained from the defendant; (b) any item that the government intends to use for its case-in-chief against the defendant; and (c) any items that are "material to preparing the defense." *See* FED. R. CRIM. P. 16(a)(1)(E), https://www.law.cornell.edu/rules/frcrmp/rule_16.

[97] "[CIPA] creates no new rights of or limits on discovery of a specific area of classified information. Rather it contemplates an application of the general law of discovery in criminal cases[.]" *United States v. Yunis*, 867 F.2d 617, 621 (D.C. Cir. 1989), https://scholar.google.com/scholar_case?case=4751659880446145244&q=867+F.2d+617&hl=en&as_sdt=80006.

[98] Along with the evidence it submits for *in camera* discoverability review, the government may submit an *ex parte* brief arguing which evidence should or should not be found discoverable.

[99] *See* CIPA § 4, codified at 18 U.S.C. App. III § 4.

[100] *Id.*

[101] If the court denies the government's request to produce substitutes of classified information, its decision may be subject to interlocutory appeal. *See id.* § 7(a).

(c) redacted documents.[102] Additionally, the government may declassify information so that it can be produced to the defendant.

C. Pretrial Admissibility Proceedings

[51] Following the discovery process, CIPA provides pretrial procedures to determine what classified information will be admissible at trial. First, the defense specifies the classified materials it expects to use at trial. This leads to a hearing at which the court determines admissibility. Then, the government can ask the court for permission to use substitutes of classified materials. If the court refuses, the government must decide to permit disclosure or suffer an adverse order.

1. The Admissibility Hearing

[52] In CIPA cases, the defense provides notice of what classified information it intends to use (or cause to be used) at trial.[103] After receiving notice from the defense, or at the request of the government, the court holds a hearing. At the hearing, the court makes "all determinations concerning the use, relevance, or admissibility of classified information that would otherwise be made during the trial or pretrial proceeding."[104]

[53] Prior to the hearing, the prosecution provides the defense with notice of the classified information it considers "at issue."[105] At the hearing, held *in camera*, the parties present arguments as to which items of classified information should be admissible.[106] The court applies generally applicable evidence rules to determine what classified items are admissible as evidence.[107] Under CIPA, the court uses "existing standards for determining relevance and admissibility of evidence."[108]

[54] For each item of classified evidence the court deems admissible, the court orders the prosecution to "provide the defendant with the information it expects to use to rebut the classified information."[109] If the government fails to provide rebuttal information, it can be excluded from the trial.[110]

---

[102] *Id.* § 4.
[103] *Id.* § 5(a).
[104] *Id.* § 6(a).
[105] *See id.* § 6(b)(1).
[106] The court can excuse government lawyers from the hearing while the defense makes a proffer of its case, to avoid divulging defense strategies to the prosecution.
[107] The Federal Rules of Evidence that generally govern admissibility determinations are available at https://www.law.cornell.edu/rules/fre.
[108] *Anderson*, 872 F.2d at 1514.
[109] CIPA § 6(f), codified at 18 U.S.C. App. III § 6(f). The court may also "place the [prosecution] under a continuing duty to disclose such rebuttal information."
[110] *Id.* ("If the [prosecution] fails to comply with its obligation [to provide rebuttal information], the court may exclude any evidence not made the subject of a required disclosure and may prohibit the examination by the [prosecution] of any witness with respect to such information.").

2. Government Requests to Use Substitutes

[55] Classified information the court finds to be admissible can be used as evidence at trial, and thus publicly disclosed. However – as in the discovery stage – CIPA permits the government to argue that national security requires using substitutes of classified materials that have been deemed admissible.[111]

[56] The court may permit government-offered substitutes to be used in lieu of original materials if it finds they "will provide the defendant with substantially the same ability to make his defense as would disclosure of the specific classified information" at issue.[112] CIPA anticipates substitutes such as (a) written summaries of classified information; (b) admissions of or stipulations to facts classified information would prove; or (c) documents where non-relevant classified information has been redacted.[113]

3. The Government's Right to Block Disclosure, and Mandatory Sanctions

[57] The court may find that a government-proffered substitute will not provide defendants with an adequate ability to defend themselves, and may thus deny the government's request to use substitute evidence.[114] If so, the defense has the right to disclose the classified material without alteration by presenting it as evidence at trial.

[58] In such situations, CIPA provides that the government decides whether it will permit classified materials to be disclosed, or block disclosure and suffer the consequences. If the government decides to let the defense disclose classified information, the case proceeds to trial. Alternatively, the government can block the disclosure of classified evidence. To do so, the US Attorney General files an affidavit objecting to the use of classified information; in that event, the court orders "that the defendant not disclose" the objected-to materials.[115]

[59] If the government objects to the use of classified information in this fashion, CIPA requires the court to dismiss the criminal proceedings unless it finds that "the interests of justice would not be served by dismissal."[116] If it finds the latter, the court enters an alternative: (a) dismissal of specific charges brought against the defendant; (b) conclusively resolving issues of fact against the government; or (c) striking all or part of a government witness's testimony.[117]

---

[111] *Id.* § 6(c).
[112] *Id.* § 6(c)(1).
[113] *See id.* §§ 6(c)(1), 8(b).
[114] When the court requires the government to let the defendant use classified information without alteration, the government may have a right to an expedited interlocutory appeal. Section 7(a) of CIPA permits interlocutory appeals when the trial court has entered an order "authorizing the disclosure of classified information." *Id.* § 7(a).
[115] *Id.* § 6(e)(1).
[116] *Id.* § 6(e)(2).
[117] *Id.* § 6(e)(2)(A)-(C). The court may also enter any sanction "the court determines is appropriate." *Id.* When the court enters sanctions, it must grant the government an opportunity to (a) seek an expedited interlocutory appeal, and to (b) withdraw its objection to the use of classified information at trial.

[60] In summary on CIPA, criminal defendants benefit from the statute's clear procedures for the treatment of classified information. Defendants retain their right to defend themselves in this process, even against classified evidence, and under full judicial supervision.